SECURITY COUNCIL REPORT
Independent. Impartial. Informative.

Research Report

Maintaining International Peace and Security in the Age of Rapid Technological Change: Is the Security Council Wired for Purpose?

Members of the Security Council screen a virtual reality project prior to the Security Council meeting on the situation in Sudan and South Sudan.
UN Photo/Manuel Elías

2026, No. 2
27 March 2026

This report is available online at **securitycouncilreport.org**.

For daily insights by SCR on evolving Security Council actions please subscribe to our **"What's In Blue"** series at securitycouncilreport.org or follow us on X: **@SCRtweets** and LinkedIn: Security Council Report

Executive Summary

Rapid advances in information and communications technology (ICTs), artificial intelligence (AI) and other emerging technologies are reshaping conflict dynamics and the broader landscape of international peace and security. As technological convergence accelerates, risks are becoming more complex, interconnected, and difficult to anticipate. The impact of technological change is increasingly visible across issues already before the Security Council, including counter-terrorism, sanctions, peacekeeping, the protection of civilians, and women, peace and security. Yet Council engagement remains limited, fragmented, and politically contested.

The report clarifies the Charter foundations for Council engagement, situates that role within the wider UN system, traces the evolution of Council practice, examines how technological developments intersect with existing thematic agenda items, analyses the divisions that have inhibited engagement, and sets out options for strengthening the Council's role.

It finds that the Council cannot afford to ignore the impact of ICTs, AI, and other new and emerging technologies. Their peace and security implications are becoming increasingly pertinent to the

2 Introduction
3 Section I: Key Concepts and Working Definitions
3 Defining ICTs, Cyberspace, and Cybersecurity
5 Artificial Intelligence
5 Other New and Emerging Technologies
6 The Challenges of Addressing New and Emerging Technologies
7 Section II: Charter Foundations and UN Processes
7 Charter Foundations for Security Council Engagement on ICTs and New and Emerging Technologies
8 General Assembly Processes on ICT Security
9 Section III: The Evolution of Security Council Engagement on ICTs and New and Emerging Technology
10 Thematic Meetings on ICTs and New and Emerging Technologies
12 Country-Specific Correspondence and Meetings on ICT-related Incidents
13 Security Council Thematic Products on Technology
14 International Law and Cyber Operations
15 Section IV: Mapping Technology Issues Across Security Council Agenda Items
15 Technology and Counter-terrorism
18 Technology and the Protection of Civilians
23 Technology and Sanctions
25 Technology and Peacekeeping
29 Technology and Women, Peace and Security
30 Section V: Member State Dynamics on the Security Council's Role
30 Dynamics among Member States on the Council's Role in Addressing Cyber Threats
33 Dynamics among Member States on the Council's Role in Addressing AI and New and Emerging Technologies
35 Section VI: Options for Security Council Engagement on ICTs and New and Emerging Technologies
35 Options for Security Council Members
38 Options for Non-Council members and the Broader UN Membership
40 Options for the UN Secretariat
41 Options for Non-Governmental Organisations and the Private Sector
43 Annex I: Security Council Thematic Meetings on Technology (2016-2025)
45 Annex II: Preliminary Aide Memoire on Technology

Executive Summary

Council's work, not only as sources of risk but also as potential enablers of more effective analysis and operational support, including in sanctions monitoring and implementation and in enhancing the effectiveness of UN peacekeeping. However, divisions among member states, particularly the permanent members, have constrained the development of a shared approach and limited agreement on formal products. The result is a growing gap between the speed of technological change and the pace of the Council's institutional adaptation.

Three conclusions stand out. First, more systematic Council engagement is needed. The peace and security implications of these technologies are already increasingly evident across the Council's work, and there is growing recognition that, as these technologies expand in scale and complexity, their implications for the maintenance of international peace and security are likely to become more pronounced. The question is therefore less whether these issues belong on the Council's agenda than how they can be addressed more consistently and effectively across existing thematic and country-specific practice.

Second, more systematic Council engagement should be pursued in complementarity with other intergovernmental processes addressing the security implications of specific technologies, including the Global Mechanism on ICT security. A complementary approach would allow the Council to draw on existing normative frameworks while focusing on the specific peace and security dimensions that fall within its mandate.

Third, technological change cannot be approached solely through a reactive lens. The peace and security implications of new and emerging technologies may become fully visible only once systems are deployed at scale, by which point the risks may be harder to contain. Anticipation is therefore essential.

Although Council dynamics continue to complicate more systematic engagement, a range of stakeholders can still help strengthen Council practice. The report recommends establishing an Informal Expert Group on Technology, Peace and Security to support more sustained engagement and help mainstream these issues across existing agenda items, alongside a voluntary commitments initiative to sustain attention to the topic. It also recommends strengthening Security Council-General Assembly complementarity, including through Groups of Friends and more regular exchanges with the new Global Mechanism. In addition, it proposes that the Secretariat develop a technology aide memoire to improve continuity and track agreed language, and make fuller use of existing working methods to ensure that significant cyber incidents and other technology-related threats can still be raised when formal discussion proves difficult. Finally, it recommends establishing a multi-stakeholder working group to support coordination, analysis, and information-sharing.

The report concludes that the Security Council is not yet wired for purpose. As technological change increasingly shapes the risks and opportunities to international peace and security, however, the question is no longer whether the Council can afford to engage more systematically on these issues. It is whether it can afford not to.

Introduction

The United Nations was created at the dawn of the atomic age, when scientific progress had revealed its capacity not only to transform human life but also to threaten humanity on an unprecedented scale. From the outset, the organisation was therefore shaped by a central question that remains relevant to this day: how should the international community respond when technological change alters the conditions of international peace and security? That question is acquiring renewed urgency.

Today, threats to international peace and security may arise not only from conventional military action but also through a line of code, an algorithmic process, or an autonomous action. Information and communication technologies (ICTs) and new and emerging technologies, including artificial intelligence (AI), are reshaping the parameters of peace and security, influencing both the nature of conflict and the means by which it is prevented and managed.

The Security Council, which bears primary responsibility for the maintenance of international peace and security, must decide how it will engage with the challenges and opportunities such technologies present in the discharge of its responsibilities. As cyber threats and the risks associated with AI and other new and emerging technologies continue to expand in scale and complexity, these issues are likely to assume greater significance in the Council's deliberations and decisions.

This report examines the Security Council's engagement on issues related to ICTs and new and emerging technologies. It analyses the Council's practice, including how these technologies have been addressed in thematic deliberations, how they have been reflected in country-specific situations, and how member states have discussed their relevance to the Council's mandate. The report also maps the intersections between the risks and opportunities associated with these technologies and existing thematic items on the Council's agenda. Finally, it considers the practical and political constraints that have shaped the Council's engagement and, in light of these factors, explores options for future action.

This report is divided into six sections:

- Section I introduces key concepts and working definitions on ICTs, AI, and other new and emerging technologies, and outlines the distinct challenges these technologies pose for international peace and security and for the Council's work.
- Section II examines the Charter foundations for Security Council engagement on ICTs and new and emerging technologies and situates that role within the broader UN landscape, particularly the General Assembly processes on the security of and in the use of ICTs.
- Section III traces the evolution of the Council's engagement on technology, examining thematic and country-specific practice on ICTs, AI, and other new and emerging technologies, and the political and legal divisions that have limited agreement on thematic products.
- Section IV maps the intersections between ICTs and new and emerging technologies, including AI, and the Council's thematic agenda items, including counter-terrorism, protection of civilians, sanctions, peacekeeping, and women, peace and security, highlighting both areas of growing integration and areas where engagement remains fragmented or contested.
- Section V analyses the dynamics shaping Council engagement on ICTs and new and emerging technologies, highlighting divisions over the Council's role, questions of complementarity with General Assembly processes, and the constraints these divisions have placed on more systematic engagement.
- Section VI sets out options for strengthening the Council's engagement on ICTs, AI, and other new and emerging technologies, drawing on existing practice, working methods, and precedents, and organising the recommendations by stakeholder: Council members, the wider UN membership, the UN Secretariat, and non-governmental organisations and the private sector.
- The annexes include a list of Security Council meetings specifically focused on technology-related issues, as well as a preliminary aide memoire on technology compiling agreed language from Council products by thematic issue and, where relevant, by country situation.

Section I: Key Concepts and Working Definitions

Defining ICTs, Cyberspace, and Cybersecurity

The term "cyber" is broadly used to describe matters relating to computers, digital technologies, and networked communication. It often serves as a prefix for activities, systems, and threats that operate through, target, or depend on the digital environment commonly referred to as "cyberspace". Cyberspace, in turn, refers to the virtual environment of interconnected digital devices and networks in which digital communication, data exchange, and online interaction take place.

Understanding how cyberspace functions requires some familiarity with information and communications technologies (ICTs), a broad term referring to technologies used to collect, process, store, and transmit information.[1] The UN Convention against Cybercrime defines an ICT system as "any device or group of interconnected or related devices, one or more of which, pursuant to a program, gathers, stores and performs automatic processing of electronic data".[2] This formulation closely mirrors the definition of a "computer system" in the Council of Europe Convention on Cybercrime (Budapest Convention).[3] In practical terms, ICTs comprise the tools and systems that underpin everyday digital services, enabling individuals and organisations to access, share, and manage information through networked systems such as the Internet.

The Internet is the most widely used global network for accessing and interacting within cyberspace.[4] It consists of interconnected networks, computers, and devices that enable communication, access to websites, and the transmission and sharing of data. While often conflated with cyberspace, the Internet is only one component of the broader digital environment constituted by interconnected ICT systems and networks. An extension of this ecosystem is the Internet of Things (IoT), which refers to networks of physical devices, such as smart appliances, sensors, vehicles, and industrial equipment, that are connected to networks, including the Internet, and capable of collecting and exchanging data. Through IoT, digital functionality is increasingly embedded in homes, workplaces, and public infrastructure.[5]

[1] These include devices such as computers and smartphones, as well as software, communication networks, and data storage infrastructure.

[2] UN Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes (2024); UN Office on Drugs and Crime (UNODC) Press Release. "UN Convention against Cybercrime Opens for Signature in Hanoi, Viet Nam". (25 October 2025). The convention was signed by 72 states at its opening for signature in Hanoi, Viet Nam on 25-26 October 2025.

[3] This Convention defines "computer system" as "any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data".

[4] Approximately 6 billion people, or about three-quarters of the world's population, were connected to the Internet in 2025. See United Nations (19 November 2025). "Progress and Gaps: Key Findings from ITU's Facts and Figures 2025".

[5] Industry estimates projected the number of connected IoT devices would exceed 21 billion by the end of 2025. See Satyajit Sinha (28 October 2025)."State of IoT 2025: Number of connected IoT devices growing 14% to 21.1 billion globally". IoT Analytics.

Against this backdrop of growing interconnectivity and reliance on digital systems, cybersecurity has assumed heightened importance. The term is generally understood to refer to the protection of digital systems, networks, and data from unauthorised access, disruption, or destruction.[6] It is related to, but distinct from, efforts to combat cybercrime, which focus primarily on preventing and responding to criminal activity conducted through ICTs, including fraud, exploitation, and other offences that often affect individuals and private entities. In technical terms, cybersecurity is often framed through the principles of confidentiality, integrity, and availability of ICTs. In policy and security contexts, it also carries broader implications for national security and international stability, including the protection of critical infrastructure such as power grids, healthcare systems, transportation networks, and financial institutions that are increasingly dependent on ICTs.

Within multilateral discussions, some states adopt a broader framing, often using the term "information security" to encompass not only the protection of ICTs but also risks associated with content disseminated through digital means. This approach places greater emphasis on securing the information environment against manipulation and influence operations aimed at shaping public opinion, amplifying divisions, or affecting political outcomes, with potential implications for social cohesion, political stability, and national security. In this regard, ICT-related discussions are often linked to notions of information sovereignty and the role of the state in regulating national information spaces.

In recent years, malicious cyber activity has affected a wide range of sectors, including energy infrastructure, healthcare services, humanitarian operations, government institutions, election systems, and nuclear facilities. Cyber operations conducted in the context of armed conflict are sometimes described as "cyberattacks". They may also form part of broader "hybrid warfare" strategies, a term occasionally used within Security Council deliberations to describe the integration of cyber capabilities with conventional, economic, and informational tools to advance strategic objectives while remaining below the threshold of traditional armed conflict.[7]

The Challenges of Addressing Cyber Threats

Addressing malicious ICT activity presents challenges that differ in important respects from those posed by conventional threats. ICTs are ubiquitous, widely available, and neither inherently civilian nor military in nature. Many of the tools used in cyber operations are also relatively inexpensive and often open source, lowering barriers to entry and enabling a broad range of actors, including non-state groups and individuals, to acquire capabilities to conduct malicious cyber activity. As a result, the cyber threat landscape may be more crowded and less predictable than traditional military domains.[8]

A second challenge stems from the nature of cyberspace itself. Unlike land, sea, air, or space, cyberspace is a human-made environment operated and maintained by a wide range of actors, including governments, private companies, civil society, and individual users. Much of the underlying infrastructure is privately owned, making the private sector central to both the functioning and the security of the digital environment. This overlap of public and private roles can complicate coordination, regulation, and the implementation of agreed norms.

Another challenge is that malicious cyber activity can often be concealed. The origin of an operation, the identity of the perpetrator, and the motive behind it may be difficult to ascertain. Actors may seek to obscure their location or identity through techniques such as encryption, proxy servers, virtual private networks, IP spoofing, and botnets, while false-flag techniques may further complicate investigation.[9] Cyber operations may also be conducted remotely, rapidly, and in some cases without warning, leaving little time for detection or mitigation. Unlike many conventional military operations, which may involve observable indicators such as troop movements, malicious cyber activity can be executed at speed and with limited visibility, constraining the ability to respond in real time.

These features make attribution one of the most difficult aspects of responding to malicious cyber activity. Digital evidence is often dispersed across multiple countries and jurisdictions, while investigative processes are highly technical, resource-intensive, and not infallible. Although many states have developed digital forensic capabilities, these vary significantly, and even where an operation can be linked to a particular device or network, this may still not reveal who ordered, directed, or supported it. In practice, perpetrators may therefore operate across borders with substantial impunity, particularly where states lack the technical, legal, or institutional capacity to investigate effectively.[10]

Establishing state responsibility under international law in relation to malicious ICT activity is similarly complex. Identifying the individual or group involved is not, in itself, sufficient. States must also demonstrate a clear and compelling connection to the conduct in question, whether through direct control, funding, operational support, or, at a minimum, awareness and tolerance of the activity occurring within their territory. States have agreed that they should not knowingly allow their territory to be used for internationally wrongful acts using ICTs, a principle reflected in the General Assembly-endorsed norms of responsible state behaviour in cyberspace.[11]

At the same time, the evidentiary threshold many states apply before publicly attributing malicious cyber activity to another state is often high, given the potential diplomatic, legal, and security consequences. States may therefore be reluctant to make attributions public unless they are confident in both the underlying technical evidence and the legal basis for doing so.[12]

The digital divide adds a further layer of difficulty. As digitalisation

[6] The International Telecommunication Union (ITU) defines cybersecurity more specifically as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user's assets. Organisation and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment". See: ITU Recommendation ITU-T X.1205, Overview of Cybersecurity.

[7] On 31 March 2017, during its second year as an elected member of the Security Council, Ukraine convened an Arria-formula meeting on hybrid wars as a threat to international peace and security. The meeting's concept note defined "hybrid warfare" as "the employment of a combination of military, quasi-military and non-military instruments in a synchronised manner tailored to specific vulnerabilities of the target", identifying cyber technologies as one of the means used to achieve political objectives. See Security Council Report, "Arria-formula Meeting on Hybrid Wars", What's in Blue (30 March 2017).

[8] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (30 July 2010) (A/65/201).

[9] Andraž Kastelic (2022). Non-Escalatory Attribution of International Cyber Incidents: Facts, International Law and Politics, Geneva, Switzerland: UNIDIR.

[10] Ibid.

[11] Final Report of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025 (24 July 2025) (A/80/257).

[12] Andraž Kastelic (2022). Non-Escalatory Attribution of International Cyber Incidents: Facts, International Law and Politics, Geneva, Switzerland: UNIDIR.

expands, states with limited resources and constrained technical capacity may be more vulnerable to malicious cyber activity and may lack the expertise, institutional capacity, or financial means to put effective defences in place. Environments with weak security measures may also be exploited as operational bases by malicious actors. Limited oversight, outdated systems, and jurisdictional gaps can allow cross-border cyber operations to be launched from within a state's territory without the knowledge or consent of the relevant authorities. These dynamics have led many observers to characterise global cybersecurity as being only as strong as its weakest link.[13] Against this backdrop, member states have repeatedly stressed that capacity-building is a fundamental component of international cooperation in cyberspace.[14] Strengthening national and regional resilience has therefore become a central focus of multilateral discussions on ICT security.

Artificial Intelligence

There is no universally agreed definition of AI. In UN usage, however, the term generally refers to systems designed and trained to learn, solve problems, make predictions, take decisions, and perform tasks regarded as requiring a level of intelligence comparable to that of a human.[15] AI encompasses several subfields, including machine learning, natural language processing, and computer vision.

The UN Conference on Trade and Development describes AI as developing in three broad waves.[16] Early systems were largely rule-based, operating through predefined instructions and decision trees. Later advances in statistical learning and machine learning enabled so-called narrow or weak AI, capable of performing specific tasks, such as classification, recognition, or prediction, within limited domains. The current wave is shaped by generative AI, driven by advances in natural language processing, large language models (LLMs), and computing power, and capable of producing new content, including text, code, images, video, and audio.[17] A further development is the emergence of AI agents that can reason, plan, and pursue user-defined goals through multi-step actions, including by using external tools, software, or other systems, rather than simply generating a single output in response to a prompt. The rapid expansion of generative AI has renewed discussion of hypothetical artificial general intelligence (AGI) and artificial superintelligence, which would surpass human capabilities altogether.[18]

AI poses a growing range of risks for international peace and security. As increasingly capable systems become more accessible, AI may lower barriers to entry for both state and non-state actors seeking to conduct malicious activity. States have warned that it could facilitate cyberattacks, including against critical infrastructure; enable the rapid production and dissemination of synthetic content, misinformation, and disinformation; and lower the cost and expertise required for the development of biological weapons.[19]

In the military domain, AI is already being integrated into targeting, decision-support systems, autonomous systems, and weapons platforms. This has heightened concerns about lethal autonomous weapons systems (LAWS), the erosion of meaningful human control, and compliance with international humanitarian law. One of the central concerns associated with advanced AI systems is their opacity.[20] Many operate as "black boxes", making it difficult to understand how particular outputs were produced and thereby complicating oversight and accountability in high-stakes settings.[21]

More broadly, AI may intensify strategic competition over the key inputs needed to develop and deploy it, including chips, data, and critical minerals. It may also leave many states dependent on infrastructure and technical standards controlled by a small number of states and firms, a dynamic sometimes described as a form of "cyber colonization".[22] AI also expands the scope for mass surveillance, behavioural monitoring, and social control. Beyond the security sphere, it may disrupt labour markets, concentrate economic and political power, and add to environmental and climate pressures through its substantial energy, water, and material demands.[23] UN advisory processes have also highlighted the possibility of more extreme risks associated with AGI or superintelligence, including scenarios involving uncontrollable or uncontainable systems, or systems no longer meaningfully attributable to human, corporate, or state actors.[24]

At the same time, AI also offers important opportunities relevant to peace and security. It may strengthen ICT security by helping detect intrusions and other malicious activity, including against critical infrastructure; support the identification of AI-generated misinformation, disinformation, and hate speech; improve situational awareness, risk mitigation, and de-escalation; and assist peacekeeping, ceasefire monitoring, disarmament verification, counter-terrorism, and humanitarian response. Some states have also suggested that it could support the implementation of international humanitarian law, including the principles of distinction, proportionality, and precautions in attack, as well as the protection of civilians and civilian objects.[25]

Other New and Emerging Technologies

The term "new and emerging technologies" is generally used in the UN as a broad, context-dependent umbrella category, usually demonstrated through examples rather than defined by fixed criteria. The Secretary-General's 2018 Strategy on New Technologies, for

[13] ITU (2008). Global Cybersecurity Agenda: Global Strategic Report, Geneva, Switzerland: ITU.

[14] Final Report of the Open-ended Working Group on Security of and in the Use of Information and Communications technologies 2021–2025 (24 July 2025) (A/80/257).

[15] Report of the Secretary-General on Current Developments in Science and Technology and their Potential Impact on International Security and Disarmament Efforts (22 July 2025) (A/80/237).

[16] UNCTAD. Technology and Innovation Report: Inclusive Artificial Intelligence for Development (2025).

[17] Some have highlighted the cross-border risks associated with their use, including for implementing malicious cyber operations. See Talita Dias. Governing AI Agents Globally: The Role of International Law, Norms and Accountability Mechanisms. Just Security (17 October 2025).

[18] In this regard, "singularity" is commonly used to refer to the point at which rapidly advancing technology produces an AI that surpasses human intelligence and operates beyond our control. See, for example, Nicholas Wright. AI & Global Governance: Three Distinct AI Challenges for the UN. UNU-CPR (7 December 2018).

[19] Report of the Secretary-General on Artificial Intelligence in the Military Domain and Its Implications for International Peace and Security (5 June 2025) (A/80/78); See also Eleonore Pauwels. How can Multilateralism Survive the Era of Artificial Intelligence? UN Chronicle. December 2018, Nos. 3 & 4 Vol. LV, "New Technologies: Where To?" (21 December 2018).

[20] Ibid.

[21] UN Office of Information and Communications Technology. "Emerging Technologies".

[22] Eleonore Pauwels (2019). The New Geopolitics of Converging Risks: The UN and Prevention in the Era of AI, UN University Centre for Policy Research (UNU-CPR).

[23] UNCTAD. Technology and Innovation Report: Inclusive Artificial Intelligence for Development (2025).

[24] Governing AI for humanity (2024)

[25] Report of the Secretary-General on Artificial Intelligence in the Military Domain and Its Implications for International Peace and Security (5 June 2025) (A/80/78).

example, refers to technologies such as AI, biotechnology, blockchain, and robotics. Work under the UN's Technology Facilitation Mechanism similarly links "new and emerging technologies" to "rapid technology change" and "frontier technologies", describing fast-moving developments in fields such as robotics, AI, biotechnology, and nanotechnology as "disruptive technologies".[26]

For the purposes of this report, new and emerging technologies are understood as scientific and technological innovations that are novel in application, possess significant transformative potential, and may evolve faster than existing regulatory or governance frameworks can adapt. Many are dual use, developed for commercial or scientific purposes but capable of military application.[27] Commonly cited examples include AI and autonomy, quantum technologies, neurotechnology, and materials technologies.[28]

Quantum technologies apply the principles of quantum mechanics to areas such as computing, communication, and sensing. Quantum computing, while still at an early stage, is expected to transform fields that depend on advanced data processing, including cryptography, complex simulation, and AI-driven automation.[29] To illustrate this potential, Google reported in 2019 that one of its quantum processors completed a task in 200 seconds that it estimated would take a classical computer thousands of years.[30] Their growing significance was also reflected in the General Assembly's designation of 2025 as the International Year of Quantum Science and Technology.[31] From a peace and security perspective, one of the main concerns is that sufficiently powerful quantum computers could break widely used public-key encryption, with implications for critical infrastructure, sensitive government data, and military communications.[32] Conversely, quantum technologies could also strengthen cybersecurity, including through new cryptographic applications. Their implications for warfare and security nevertheless remain highly uncertain.[33] There is currently no dedicated intergovernmental process focused on quantum technologies in the context of international security, although states in ICT security discussions have noted that the evolving properties of quantum computing may create new threats and vulnerabilities.

Neurotechnology raises a different, but equally serious, set of concerns, particularly as it increasingly intersects with AI and other emerging technologies. The term refers broadly to devices and systems that interact with the nervous system, including brain-computer interfaces (BCIs), which establish a direct connection between the brain and external devices. In that sense, neurotechnology reflects a broader trend towards convergence across the digital, physical, and biological domains.[34] A key concern is that such technologies could open new pathways for surveillance, coercion, and military use, including the extraction of sensitive neural data, cyber vulnerabilities in connected devices, behavioural influence, and cognitive warfare and disinformation.[35] Recent advances across multiple fields have made the integration of neurotechnology into military contexts increasingly plausible in the near term.[36] Advances in BCIs could reportedly be used not only to augment soldiers' capabilities, but also to enable new forms of human-machine teaming on the battlefield such as mind-controlled swarms of drones.[37] These developments have raised concerns about a possible neurotechnology arms race.[38]

Additive manufacturing, or 3D printing, similarly shows how technologies with clear civilian benefits may also carry growing security risks. Alongside its potential for rapid prototyping, localised and on-demand production, and applications ranging from industrial innovation to prosthetics and other medical uses, additive manufacturing, especially when combined with open-source knowledge, can lower barriers for both state and non-state actors to produce automatic firearms and potentially hardware relevant to nuclear enrichment capabilities.[39]

The Challenges of Addressing New and Emerging Technologies

Addressing the peace and security implications of new and emerging technologies presents distinct challenges for the Security Council. Many of these technologies are advancing rapidly, with security implications that may become apparent only once they are deployed at scale. This creates a basic difficulty for a body charged with maintaining international peace and security. By the time the risks are clearly visible, they may already be harder to contain.

The pace of scientific and technological change further complicates efforts to respond. Advances in areas such as AI, autonomous systems, and quantum technologies may outstrip the capacity of existing governance and regulatory frameworks to assess and

[26] Secretary-General's Strategy on New Technologies (September 2018); UN Department of Economic and Social Affairs. "Work stream 10: Analytical work on emerging technologies and the SDGs".

[27] Wenting He (2024). Enabling Technologies and International Security: A Compendium (2024 edition), Primer, Geneva, Switzerland: UNIDIR; See also Zhanna L. Malekos Smith and Giacomo Persi Paoli (2024). Quantum Technology, Peace and Security: A Primer, Geneva, Switzerland: UNIDIR.

[28] Report of the Secretary-General on Current Developments in Science and Technology and their Potential Impact on International Security and Disarmament Efforts (23 July 2024) (A/79/224).

[29] In quantum computing, information is encoded in quantum bits, or qubits, which can exist in a superposition of 0 and 1, allowing certain problems to be processed far faster than would be possible with classical computers.

[30] CNN Business (23 October 2019). "Google claims its quantum computer can do the impossible in 200 seconds".

[31] UNESCO. "International Year of Quantum Science and Technology".

[32] Report of the Secretary-General on Current Developments in Science and Technology and their Potential Impact on International Security and Disarmament Efforts (22 July 2025) (A/80/237).

[33] Malekos Smith, Zhanna L., and Persi Paoli, Giacomo (2024). "Quantum technology, peace and security: a primer". Geneva, Switzerland: UNIDIR.

[34] Report of the Human Rights Council Advisory Committee on Impact, Opportunities and Challenges of Neurotechnology with Regard to the Promotion and Protection of all Human Rights. (8 August 2024) (A/HRC/57/61*); See also Eleonore Pauwels. How can Multilateralism Survive the Era of Artificial Intelligence? UN Chronicle. December 2018, Nos. 3 & 4 Vol. LV, "New Technologies: Where To?" (21 December 2018).

[35] Ibid.; See also Eleonore Pauwels (2019). The New Geopolitics of Converging Risks: The UN and Prevention in the Era of AI, UN University Centre for Policy Research (UNU-CPR).

[36] Federico Mantellassi and Edward Madziwa (2025). "Neurotechnology in the Military Domain: A Primer". Geneva, Switzerland: UNIDIR.

[37] Geneva Centre for Security Policy (11 April 2022). "In focus: The challenges of neurotechnology"; the Human Rights Council Advisory Committee on Impact, Opportunities and Challenges of Neurotechnology with Regard to the Promotion and Protection of all Human Rights emphasised that "the idea of introducing 'augmented soldiers' is worrying and red lines should be drawn".

[38] Federico Mantellassi and Edward Madziwa (2025). "Neurotechnology in the Military Domain: A Primer". Geneva, Switzerland: UNIDIR.

[39] Report of the Secretary-General on Current Developments in Science and Technology and their Potential Impact on International Security and Disarmament Efforts (22 July 2025) (A/80/237).

manage the risks they generate.[40] In the AI context, this challenge is often captured in the idea of a "singularity", namely the possibility that accelerating technological progress could produce systems that surpass human intelligence and move beyond human control.

These difficulties are compounded by technological convergence, through which distinct technologies interact, overlap, or become integrated in ways that amplify both their capabilities and their risks. The effects may be greater than the sum of the individual technologies involved. AI, for example, is increasingly functioning as an enabling technology in other domains. Its application in biology may support beneficial innovation in health and science, but may also assist state and non-state actors in acquiring materials and information relevant to biological weapons development.[41]

A further challenge is institutional. Although various UN bodies address specific technologies or sectors, these efforts remain fragmented. Discussions on lethal autonomous weapons systems, for example, provide one venue for examining a specific category of military technology, while First Committee consideration of the role of science and technology in the context of international security and disarmament, together with reporting by the Secretary-General, has helped draw attention to broader trends. Other disarmament bodies, including the Conference on Disarmament, similarly provide forums in which certain emerging technology issues may be raised. There is, however, no equivalent across technologies to the sustained intergovernmental work that General Assembly processes have provided on ICT security. As a result, Council members lack a single consolidated analytical basis for assessing how technological developments may affect the maintenance of international peace and security. This institutional gap limits the Council's ability to engage emerging risks posed by new technologies in a timely, coherent, and informed manner.

These factors underscore the difficulty the Council is likely to face in responding effectively to the peace and security implications of new and emerging technologies. Rapid technological change, converging risk pathways, and institutional fragmentation all complicate early warning and timely action. They also suggest that a reactive approach will often be insufficient. If the Council is to engage meaningfully with these risks, it will need to do so in a more anticipatory manner, before potential harms crystallise into more concrete threats. This was part of the logic underpinning efforts by Switzerland and other members in 2024 to encourage the Council to take scientific developments into account more systematically through a preventive lens.[42] Yet efforts to secure more operational follow-through, including analytical reporting by the Secretary-General on these issues, have not succeeded. How the Council might nevertheless operationalise a more anticipatory approach to emerging technologies therefore remains an open question, and one that subsequent sections of this report examine further.

Section II: Charter Foundations and UN Processes

Charter Foundations for Security Council Engagement on ICTs and New and Emerging Technologies

The Charter is widely understood to be technology-neutral. Its key provisions relevant to international peace and security are framed in terms of effects and consequences rather than the particular means through which they occur. Article 2(4), for example, prohibits the threat or use of force against the territorial integrity or political independence of any state without reference to specific weapons or methods. The International Court of Justice has similarly observed that the Charter's rules governing the use of force apply "to any use of force, regardless of the weapons employed".[43] This reflects a general understanding that the Charter's fundamental principles remain applicable as technologies evolve.[44]

Article 24(1) of the UN Charter provides that member states confer on the Security Council primary responsibility for the maintenance of international peace and security and agree that, in carrying out this responsibility, the Council acts on their behalf. This provides the legal and institutional basis for the Council's engagement on threats to peace and security. In practice, the Council's understanding of what may constitute such a threat has evolved over time, extending beyond inter-state armed conflict to encompass a broader range of situations.[45]

In support of this role, the Charter entrusts the Council with functions relating both to the pacific settlement of disputes under Chapter VI and to the identification of, and response to, threats to the peace, breaches of the peace, and acts of aggression under Chapter VII. Under Article 34, the Council may investigate "any dispute, or any situation which might lead to international friction or give rise to a dispute" in order to determine whether its continuation is likely to endanger international peace and security. In the cyber context, such disputes or situations could potentially include disagreements between states over the attribution, legal characterisation, or effects of a cyber operation, or broader patterns of hostile cyber activity that may affect international peace and security.[46]

Chapter VII provides the Council with further authority where it determines, under Article 39, the existence of a threat to the peace, a breach of the peace, or an act of aggression. Council practice indicates that a "threat to the peace" extends beyond circumstances

[40] Report of the Secretary-General on Artificial Intelligence in the Military Domain and Its Implications for International Peace and Security (5 June 2025) (A/80/78).

[41] Report of the Secretary-General on Current Developments in Science and Technology and their Potential Impact on International Security and Disarmament Efforts (22 July 2025) (A/80/237).

[42] S/PRST/2024/6 (21 October 2024).

[43] Advisory Opinion of the International Court of Justice on the Legality of the Threat or Use of Nuclear Weapons (1996), ICJ Report.

[44] This general approach is also reflected in subsequent legal and normative instruments, which tend to refer to categories of means in broad terms rather than specifying specific tools or technologies. The General Assembly's Definition of Aggression, for example, includes "the use of any weapons by a State against the territory of another State", while the Friendly Relations Declaration reiterates the prohibition contained in Article 2(4) without tying it to particular means.

[45] The Council has, for example, addressed transnational terrorism, climate-related security risks, and certain public health emergencies, among other issues.

[46] T. de Souza Dias (2021). Applying Chapters VI and VII of the Charter of the United Nations in the Cyber Context: The Challenges and Opportunities of Information and Communications Technologies, Geneva, Switzerland: UNIDIR.

involving armed force or physical violence alone.[47] The Council's treatment of public health emergencies, for example, reflects this broader understanding.[48] At the same time, the Council's determinations under Articles 34 and 39 are fundamentally political rather than strictly legal in character. This gives the Council considerable latitude to assess the scale, implications, and peace and security significance of a given situation, including those involving cyber operations or other forms of conflict driven by new technologies.

Chapter VII may also be read as broad enough to encompass certain cyber-related measures. Article 41 provides a non-exhaustive list of measures not involving the use of armed force and refers to the "complete or partial interruption of rail, sea, air, postal, telegraphic, radio, and other means of communication". This language has been cited as providing at least textual support for Security Council measures affecting digital communications and networked systems, which could be perceived as coming under the other means of communication, even though the Charter does not address cyber activity expressly.[49] A more difficult question arises in connection with Article 42, which authorises enforcement action "by air, sea, or land forces" if the Council considers that measures under Article 41 would be inadequate or have proved inadequate. While a strictly textual reading might suggest that Article 42 is framed in terms of the traditional physical domains, it has also been argued that its object and purpose may support a broader reading, under which the Council could authorise such forcible measures as may be necessary to maintain or restore international peace and security, including, where relevant, through cyber means.

Member states have reaffirmed in successive consensus reports of the Group of Governmental Experts and the Open-ended Working Group that international law, including the UN Charter, applies to state activities conducted in cyberspace.[50] Related affirmations have also been made in discussions of other technologies. In the context of lethal autonomous weapons systems, for example, the Convention on Certain Conventional Weapons (CCW) - Group of Governmental Experts has affirmed that international law, in particular the UN Charter and international humanitarian law, should guide its work.[51] General Assembly resolutions on AI in the military domain have similarly proceeded on the basis that international law, including the UN Charter, international humanitarian law, and international human rights law, applies throughout the entire life cycle of AI capabilities and the military systems they enable.[52] Together, these developments support the view that existing legal frameworks remain relevant to the use of ICTs and a broader set of new technologies with implications for international peace and security.

While the Charter may provide a legal basis for Council engagement where technological developments give rise to threats to international peace and security, the technical assessment, norm-setting, and policy work usually take place across various other UN organs and intergovernmental processes.

General Assembly Processes on ICT Security

While the Security Council bears primary responsibility for the maintenance of international peace and security, General Assembly processes have played a leading role in developing the UN's normative and institutional framework on state use of ICTs in the context of international security. Through these processes, member states have examined threats in the ICT environment and elaborated norms of responsible state behaviour, confidence-building measures, and capacity-building priorities relevant to state behaviour in cyberspace. Their outcomes have shaped the broader framework within which the Security Council may consider ICT-related risks to international peace and security.

The General Assembly's engagement on this issue dates to 1998, when it adopted a resolution introduced by Russia on "Developments in the field of information and telecommunications in the context of international security".[53] That resolution requested the Secretary-General to submit a report reflecting member states' views and assessments on information security. Since then, the item has remained on the Assembly's agenda, accompanied by periodic Secretary-General reports compiling national views on ICT-related threats and challenges.

The General Assembly deepened this work through resolution 58/32, which requested the Secretary-General to establish, in 2004, a Group of Governmental Experts (GGE) to examine existing and potential threats in the ICT environment and possible cooperative measures to address them.[54] The first GGE, composed of 15 experts appointed on the basis of equitable geographical distribution, met in 2004 and 2005 and considered the implications of ICT developments for national security and military affairs. Between 2004 and 2021, six GGEs were established.

Following the inability of the 2016-2017 GGE to agree on a consensus report, it was apparent that discussions in the General Assembly had become more challenging.[55] This divergence of views reached a pinnacle in 2018, when two separate resolutions were adopted: one, introduced by the US, establishing the sixth GGE,[56] and another, introduced by Russia, creating, for the first time, an Open-Ended Working Group (OEWG) on the issue.[57] While the two bodies had broadly similar mandates, they differed significantly in format and participation. The GGE remained a limited-membership expert process, whereas the OEWG was open to all member states.

As a result, between 2019 and 2021, the UN conducted two parallel intergovernmental processes on ICT security. As those

[47] Ibid.

[48] For example, Security Council resolution 2177 (2014) determined that the "unprecedented extent of the Ebola outbreak in Africa" constituted "a threat to international peace and security", while resolution 2532 (2020) described the COVID-19 pandemic as "likely to endanger the maintenance of international peace.

[49] Nils Melzer (2011). Cyberwarfare and International Law, Geneva, Switzerland: UNIDIR.

[50] Final Report of the Open-ended Working Group on security of and in the use of information and communications technologies 2021–2025 (24 July 2025) (A/80/257).

[51] Report of the 2019 session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems (25 September 2019) (CCW/GGE.1/2019/3).

[52] General Assembly Resolution 79/239 (24 December 2024) (A/RES/79/239).

[53] General Assembly Resolution 53/70 (4 December 1998) (A/RES/53/70).

[54] General Assembly Resolution 58/32 (8 December 2003) (A/RES/58/32).

[55] UNODA (January 2019). "Fact Sheet: Developments in the Field of Information and Telecommunications in the Context of International Security"; Samuele De Tomas Colatin (11 March 2019). "A Surprising Turn of Events: UN Creates Two Working Groups on Cyberspace", NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE).

[56] General Assembly Resolution 73/266 (22 December 2018) (A/RES/73/266).

[57] General Assembly Resolution 73/27 (5 December 2018) (A/RES/73/27).

mandates drew to a close, improving coherence between the two tracks became an objective in itself.[58] Although the GGE format was not continued after 2021, the General Assembly established a new multi-year OEWG in December 2020 for the 2021–2025 period.[59] That OEWG, chaired by Singapore, concluded its work in July 2025 with the adoption of a final report recommending the establishment of a permanent Global Mechanism to carry forward regular institutional dialogue and practical cooperation on ICT security.[60]

These GGE and OEWG processes have produced several important substantive outcomes. First, through consensus reports later welcomed and endorsed by the General Assembly, member states have repeatedly affirmed that international law, in particular the UN Charter, applies to state conduct in cyberspace.[61] These reports have also reaffirmed the relevance in the cyber context of principles including sovereign equality, the peaceful settlement of disputes, the prohibition of the threat or use of force and non-intervention in the affairs of states.[62]

Second, these processes have articulated eleven voluntary, non-binding norms of responsible state behaviour in cyberspace.[63] Among other things, these norms call on states not to conduct or knowingly support ICT activity contrary to international law that intentionally damages critical infrastructure, to take appropriate measures to protect such infrastructure from ICT threats, not to knowingly allow their territory to be used for internationally wrongful acts using ICTs, and to respond to requests for assistance from states whose critical infrastructure is subject to malicious ICT acts. While non-binding, these norms reflect important areas of political convergence.

Third, the GGE and OEWG processes have advanced confidence-building measures aimed at reducing the risks of misperception, escalation, and conflict in the cyber domain. Most notably, the 2021–2025 OEWG agreed to establish a global, intergovernmental points of contact directory for ICT security incidents to facilitate communication and information-sharing among states, including during significant cyber incidents.[64] According to the UN Office for Disarmament Affairs (UNODA), 121 states had nominated points of contact as of January 2026.

Finally, capacity-building has become a central pillar of the UN's work on the security of ICTs. Successive UN processes have highlighted persistent disparities in states' capacities to prevent, detect, and respond to malicious ICT activity, and have underscored the importance of assistance, training, and the sharing of expertise and resources, particularly for developing countries.[65] In this respect, OEWG discussions have emphasised that capacity-building is both a means of strengthening national and international resilience and a condition for the effective implementation of the broader framework for responsible state behaviour in cyberspace.[66]

Section III: The Evolution of Security Council Engagement on ICTs and New and Emerging Technology

Technology has become an increasingly visible feature of the Security Council's work, both as a cross-cutting issue arising under existing agenda items and, more recently, as a thematic subject in its own right. References to cyber threats, AI, and other new and emerging technologies have also appeared with growing frequency in broader thematic meetings held under the "Maintenance of international peace and security" agenda item, including debates on multilateralism and international law.[67]

The Council's most sustained engagement on ICTs and new technologies has historically been through its counter-terrorism agenda, where concerns about terrorists' use of the Internet and other ICT-enabled tools emerged relatively early.[68] Technology also became more prominent in discussions on UN peacekeeping, particularly as members considered how technology could enhance situational awareness, improve the protection of UN personnel, and support mandate implementation.[69] This dual framing of technology, as both an enabler and a source of risk, has remained a recurring feature of the Council's approach.

ICT security began to emerge more clearly as a thematic subject in late 2016, when Spain and Senegal convened the first Arria-formula meeting on cybersecurity and its implications for international peace and security.[70] Since then, the Council has convened 23

[58] Dan Efrony (16 July 2021). "The UN Cyber Groups, GGE and OEWG: A Consensus is Optimal, but Time is of the Essence", Just Security.

[59] General Assembly Resolution 75/240 (31 December 2020) (A/RES/75/240).

[60] Letter from the Chair of the Open-ended Working Group on its Final Report (10 July 2025) (A/AC.292/2025/CRP.1).

[61] General Assembly decision 75/564 (28 April 2021) (A/DEC/75/564).

[62] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (22 July 2015) (A/70/174); see also Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (18 March 2021) (A/75/816).

[63] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (22 July 2015) (A/70/174).

[64] Report of the Open-ended Working Group on security of and in the use of information and communications technologies 2021–2025 (8 August 2022) (A/77/275); see also UNODA, Global Intergovernmental Points of Contact Directory Portal; Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (1 August 2023) (A/78/265), Annex A: "Elements for the development and operationalization of a global, intergovernmental points of contact directory".

[65] Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (18 March 2021) (A/75/816).

[66] Letter from the Chair of the Open-ended Working Group (2021–2025), (25 June 2025).

[67] These thematic meetings include open debates and briefings held under the agenda items "Maintenance of international peace and security" and "The promotion and strengthening of the rule of law in the maintenance of international peace and security", as well as related sub-items on multilateralism, international law, leadership for peace, maritime security, and global challenges. Across these meetings, convened between 2018 and 2025, Council members and briefers have increasingly referred to cyber threats, AI, autonomous weapons systems, uncrewed aerial systems, and other emerging technologies in the context of contemporary risks to international peace and security.

[68] Security Council Resolution 1617 (29 July 2005) (S/RES/1617).

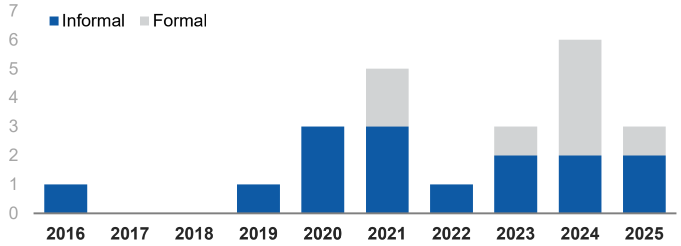
[69] Security Council Resolution 2098 (28 March 2013) (S/RES/2098); Security Council Meeting Record (11 June 2014) (S/PV.7196).

[70] Security Council Report. "Open Arria-formula Meeting on Cybersecurity". What's in Blue. (23 November 2016).

thematic meetings focused specifically on technology-related issues, with nearly two-thirds of them held in the Arria-formula format. The prominence of informal meetings reflects, in part, the political sensitivities surrounding ICT security and related topics. These meetings have helped familiarise Council members with the subject matter, facilitate exchanges with technical experts, and broaden engagement with non-Council members and other stakeholders.

Overall, the Council's engagement on ICTs and new and emerging technologies has been cautious and incremental. One reason is the absence of a dedicated agenda item or standing reporting cycle on these technologies. Consideration of these issues has therefore often depended on the initiative of individual members, whether through signature events during Council presidencies or through informal formats. As a result, engagement has tended to be sporadic and shaped by the priorities of the presidency and broader Council dynamics at a given moment.

Security Council Thematic Meetings on Technology



In recent years, however, the Council has shown a gradual evolution in its engagement. Members have increasingly convened formal meetings, including open debates and briefings, to address ICTs and new and emerging technologies during their presidencies, indicating a growing recognition by many member states of their relevance to the Council's mandate. This evolution is also evident in a shift from general discussions toward more focused consideration of specific threat vectors, including ransomware attacks against hospitals and the use of commercial spyware.

Positions among the permanent members nevertheless remain divergent. While some have supported more regular Council consideration of these issues, Russia has continued to argue, particularly on cyber threats, that the principal forum for discussion should remain the General Assembly's dedicated process.[71] In relation to AI, Russia has similarly expressed reservations about addressing the issue in the Council, including by questioning how AI, as an overarching theme, relates to the Council's mandate.[72] Nevertheless, the Council's presidential statement of 21 October 2024 indicates agreement, including among all permanent members, that scientific and technological developments warrant more systematic attention in the Council in as far as their impact on international peace and security is concerned.[73]

Thematic Meetings on ICTs and New and Emerging Technologies

Since its first dedicated meeting on cybersecurity in 2016, the Security Council's thematic engagement on ICTs and new and emerging technologies has expanded in both scope and frequency. While the Security Council has addressed ICTs and AI in separate formal meetings, broader discussions on technological change have taken place under the formulations "scientific developments" and "emerging technologies".[74]

These meetings have provided a forum for members to examine how ICTs and new and emerging technologies, including AI, intersect with the maintenance of international peace and security, often serving as an entry point for issues that had not previously received sustained attention in the Council. Even before its more regular engagement on ICTs and AI, however, the Council had addressed the security implications of other specific technologies in a more episodic manner.

One such example was the Council's engagement on unmanned aerial vehicles (UAVs)[75] in July 2019, when Peru, during its presidency, convened an informal interactive dialogue (IID) on the challenges and opportunities associated with their use.[76] The discussion focused primarily on the implications of armed UAVs for international peace and security, while also addressing unarmed applications, including in counter-terrorism contexts. It built on earlier Council consideration of UAVs, including a 2014 open debate on new trends in peacekeeping organised by Russia, which examined the use of unarmed UAVs in missions such as the UN Organization Stabilization Mission in the Democratic Republic of the Congo (MONUSCO) and the UN Multidimensional Integrated Stabilization Mission in Mali (MINUSMA).[77]

These discussions revealed differing views among member states, with some emphasising the operational benefits of UAVs for situational awareness and the protection of peacekeepers, and others raising concerns related to sovereignty, data access, and oversight.[78] While armed UAVs had previously been addressed mainly at the subsidiary level, including in the Counter-Terrorism Committee, the July 2019 IID illustrated the Council's growing willingness to explore the implications of emerging technologies more directly.

Cybersecurity as an Entry Point for Thematic Engagement

Cyber threats have been the technology-related theme most consistently addressed by the Council. Since 2016, Security Council meetings have examined issues including cyber stability, conflict prevention, and capacity-building;[79] cyberattacks targeting critical

[71] Letter from the President of the Security Council addressed to the Secretary-General and the Permanent Representatives of the members of the Security Council (1 July 2021) (S/2021/621).

[72] Permanent Mission of the Russian Federation to the UN (24 September 2025). "Statement by First Deputy Permanent Representative Dmitry Polyanskiy at a UNSC Briefing on Artificial Intelligence and International Peace and Security".

[73] Statement by the President of the Security Council (21 October 2024) (S/PRST/2024/6).

[74] See S/2021/531 (4 June 2021); S/PV.9662 (20 June 2024); S/PV.9753 (21 October 2024); and S/PV.10005 (25 September 2025).

[75] UAV refers specifically to the individual aircraft itself. In contrast, unmanned aerial system (UAS) is the broader term for the entire operational setup, including the aircraft, ground control station, the communication links, and the personnel required to control the aircraft. See UN Department of Peace Operations (DPO) and UN Department of Operational Support (DOS) (2019). Guidelines on United Nations Use of Unmanned Aircraft Systems (UAS) Capabilities.

[76] Security Council Report. "Informal Interactive Dialogue on Unmanned Aerial Vehicles (UAVs)", What's in Blue. (5 July 2019).

[77] Letter dated 1 June 2014 from the Permanent Representative of the Russian Federation to the UN addressed to the Secretary-General (A/68/899-S/2014/384).

[78] Security Council Meeting Record (23 June 2014) (S/PV.7196); UN Security Council Meeting Press Release. "Delegates Argue Merits of Unmanned Aerial Vehicles, Other Technologies as Security Council Considers New Trends in Peacekeeping". (11 June 2014) (SC/11434).

[79] Security Council Report. "Arria-formula Meeting: Cyber Stability, Conflict Prevention and Capacity Building". What's in Blue. (21 May 2020).

infrastructure;[80] and the prevention of civilian harm resulting from malicious cyber activity.[81] These meetings were often convened by elected members and typically featured briefings from technical experts and UN officials, enabling more exploratory discussions.

This engagement culminated in two high-level open debates on cyber threats, held under the agenda item "Maintenance of international peace and security" in June 2021 and June 2024, organised by Estonia and the Republic of Korea, respectively.[82] Both debates were substantively wide-ranging and provided Council members and other participating member states with an opportunity to present national priorities and broader policy positions on cyber-related topics. In doing so, they helped broaden discussion across a range of digital and emerging technology issues while further sensitising members to the implications of cyber threats for international peace and security.[83]

The Evolution of Substantive Deliberations on Cyber Threats

A comparison of the 2021 and 2024 open debates suggests a noticeable shift in emphasis over a relatively short period. The 2021 debate was focused largely on reaffirming positions already developed in the General Assembly's ICT processes. Interventions frequently stressed the applicability of international law and the UN Charter in cyberspace, the relevance of agreed voluntary norms of responsible state behaviour, and the importance of confidence-building measures and capacity-building. The debate also highlighted risks to critical infrastructure and the broader objective of preserving peace and stability in cyberspace, but gave comparatively limited attention to the practical implications of cyber threats for the Council's own work.

By contrast, the 2024 open debate featured a more practical and contextualised discussion of cyber threats and their implications for international peace and security. Many interventions referred to concrete scenarios, including cross-border cyber incidents, cyber-enabled interference in domestic affairs, and malicious cyber activities linked to armed conflict. Members also devoted greater attention to how cyber threats intersect with existing Council mandates and tools, including sanctions implementation, peace operations, counter-terrorism, the protection of civilians, and non-proliferation. The evolving threat landscape was examined in more detail as well, with particular attention to ransomware, attacks affecting healthcare and other critical infrastructure, and the role of cyber activity in heightening tensions and undermining trust between states.

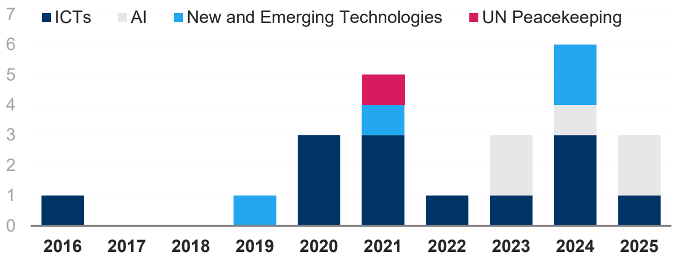
The 2024 debate also featured a more explicit discussion of the Security Council's potential role in addressing such threats. A number of member states argued that cyber threats may fall within the Council's mandate when they pose risks to international peace and security and emphasised their relevance across several agenda items. Others, while recognising a role for the Council, stressed the need to preserve a clear division of labour with General Assembly-mandated processes, particularly on the development of norms of responsible state behaviour. Together, these positions suggest that the Council was increasingly being viewed not only as a forum for broad thematic discussion, but also as a body that could help raise awareness, ease tensions, support the peaceful settlement of cyber-related disputes, reinforce agreed norms, and, in some cases, contribute to accountability in the cyber domain.

These meetings suggest that broad thematic debates have helped clarify the Council's understanding of cyber threats as they relate to its mandate, identify issues that can later be explored more closely in briefings and Arria-formula meetings, and begin to sharpen differing views on the role, if any, that the Council should play in addressing such threats.

The Growing Prominence of Artificial Intelligence

AI has recently become a more prominent focus of the Council's thematic engagement on technology. The Council first addressed the issue in a formal meeting at a July 2023 open briefing under the agenda item "Maintenance of international peace and security", organised by the UK on "Artificial intelligence: opportunities and risks for international peace and security".[84] This was followed by an Arria-formula meeting organised by Albania and the United Arab Emirates in December 2023 on "Artificial Intelligence: Its Impact on Hate Speech, Disinformation and Misinformation", and a briefing on AI under "Maintenance of international peace and security", convened by the US in December 2024.[85] In April 2025, Greece, together with France, the Republic of Korea (ROK), and several other non-Council members, organised an Arria-formula meeting on "Harnessing safe, inclusive, trustworthy AI for the maintenance of international peace and security", and, in September 2025, ROK convened the first open debate on AI. Together, these discussions highlighted both the risks associated with AI-enabled technologies and their wider societal and security implications.

Security Council Thematic Meetings by Topic (both formal and informal)



A further feature of the Council's recent engagement has been the growing overlap between discussions on cyber threats, AI, and new and emerging technologies. This reflects, in part, the open-ended nature of many thematic meetings, which has allowed members to address a wide range of issues within a single session. It also mirrors broader patterns of technological convergence, whereby advances in different technological domains increasingly interact and combine, generating compound capabilities and exposing new vulnerabilities.

[80] Security Council Report. "Arria-formula Meeting on Cyber-Attacks Against Critical Infrastructure". What's in Blue. (25 August 2020).
[81] Security Council Report. "Arria-formula Meeting on 'Preventing Civilian Impact of Malicious Cyber Activities". What's in Blue. (19 December 2021).
[82] Security Council Report. "Cybersecurity". Monthly Forecast. (June 2021); Security Council Report. "Cybersecurity". Monthly Forecast. (June 2024).
[83] UN Security Council Meeting Press Release. "Digital Breakthroughs Must Serve Betterment of People, Not Harm Them, Speakers Stress as Security Council Holds Open Debate on Cybersecurity". (20 June 2024) (SC/15738).
[84] Security Council Meeting Record (18 July 2023) (S/PV.9381); see also Letter dated 17 July 2023 from the Permanent Representative of the United Kingdom of Great Britain and Northern Ireland to the UN addressed to the Secretary-General (S/2023/528).
[85] Security Council Report. "Arria-formula Meeting on 'Artificial Intelligence: Its Impact on Hate Speech, Disinformation and Misinformation". What's in Blue. (19 December 2023).

As a result, Council discussions on AI have often touched on ICT-related issues such as online misinformation and disinformation, digital surveillance, and AI-designed malware, while discussions on ICTs have increasingly referred to AI as a factor shaping the threat landscape. These dynamics have contributed to a more integrated, albeit less clearly bounded, pattern of thematic engagement.

Country-Specific Correspondence and Meetings on ICT-related Incidents

Alongside the Council's growing thematic engagement on ICTs, member states have increasingly used letters to the President of the Security Council, the Secretary-General, and occasionally the General Assembly to draw attention to alleged cyber incidents, disinformation campaigns, and other malicious cyber activity by state and non-state actors. These communications often describe incidents affecting government infrastructure, electoral processes, critical services, and communications networks, and frequently include explicit or implicit attribution to other states.

In September 2025, for example, Moldova denounced what it described as "unprecedented Russian hybrid warfare" in the context of its parliamentary elections, alleging cyberattacks, disinformation campaigns, propaganda, and political manipulation.[86] Russia has similarly used correspondence to accuse other states, primarily the US, of orchestrating more than 12 million cyberattacks against the official website of its Central Election Commission.[87] In September 2022, Albania informed the Council that it had severed diplomatic relations with Iran following what it described as a "heavy cyber-attack" against its government's digital infrastructure,[88] an allegation Iran categorically rejected.[89] Other letters have focused on non-state actors, including Syria's March 2025 communication alleging a systematic misinformation campaign and repeated cyberattacks by armed groups reportedly supported by external parties.[90]

Several communications have also linked cyber operations to broader regional tensions and armed conflict. Lebanon, for example, has repeatedly accused Israel of cyber operations violating its sovereignty, including interference affecting the safety of civil aviation and navigation-related systems.[91] In September 2024, Lebanon further alleged a large-scale cyberattack involving the remote detonation of communication devices that caused significant civilian casualties.[92] Iran, for its part, has submitted multiple letters recalling past cyber operations against its critical infrastructure, including the Stuxnet and Duqu attacks targeting nuclear facilities, and attacks affecting its industrial infrastructure, including in the steel and petrochemical sectors, attributing such activity to Israel with support from the US.[93]

Despite the growing volume and severity of these allegations, few such communications explicitly invoke Article 39 of the UN Charter, under which the Security Council may determine the existence of a "threat to the peace, breach of the peace, or act of aggression" as a basis for measures under Chapter VII. In the above-mentioned examples cited, none characterise the incidents as a "use of force" under Article 2(4) or an "armed attack" within the meaning of Article 51, although some use related language, including references to threats to national security and to violations of sovereignty and territorial integrity. Nor have states generally asked the Council to convene specifically to address the incident in question. The overall pattern is one of cautious legal characterisation. States describe major cyber incidents as serious and destabilising and as implicating sovereignty and security, while stopping short of the Charter thresholds most directly associated with forcible action or self-defence. Nevertheless, many such incidents could plausibly be characterised as disputes, or as situations likely to lead to international friction, within the meaning of Article 34. The absence of Article 39 language, therefore, does not necessarily preclude Council competence.

To date, however, the Council's thematic engagement on cyber threats has not translated into routine or systematic consideration of cyber-related issues in country-specific situations. A notable example is the Council's discussion of Georgia on 5 March 2020 under the "Any other business" (AOB) agenda item, following a 21 February 2020 letter to the President of the Security Council describing a large-scale cyberattack in October 2019 affecting government institutions, courts, media outlets, and private sector entities.[94] In its letter, Georgia called on the international community to react appropriately, although it did not formally request that the Council meet on the incident.

Georgia subsequently approached some Council members informally about the possibility of raising the matter in the Council. There appears to have been an initial discussion among members about whether to convene an open briefing or instead raise the issue in a closed AOB discussion. It appears that, given the scale of the cyber incident and broader reservations about holding an open meeting, members settled on an AOB discussion. Afterward, the three Council members that convened it—Estonia, the UK, and the US—delivered a joint press stakeout attributing the cyberattack to Russian military intelligence agencies and characterising it as part of a broader pattern of malign activity.[95] Russia rejected the allegation, stating that no evidence had been provided.[96] Although the

[86] Identical letters dated 15 September 2025 from the Permanent Representative of the Republic of Moldova to the UN addressed to the Secretary-General and the President of the Security Council (A/80/378–S/2025/578).

[87] Letter dated 29 April 2024 from the Permanent Representative of the Russian Federation to the UN addressed to the Secretary-General (A/78/863).

[88] Identical letters dated 9 September 2022 from the Permanent Representative of Albania to the UN addressed to the Secretary-General and the President of the Security Council (A/76/943–S/2022/677).

[89] Letter dated 10 September 2022 from the Permanent Representative of the Islamic Republic of Iran to the UN addressed to the Secretary-General and the President of the Security Council (S/2022/685).

[90] Letter dated 14 March 2025 from the Permanent Representative of the Syrian Arab Republic to the UN addressed to the Secretary-General and the President of the Security Council (S/2025/152).

[91] Identical letters dated 30 July 2024 from the Chargé d'affaires a.i. of the Permanent Mission of Lebanon to the UN addressed to the Secretary-General and the President of the Security Council (A/78/975–S/2024/566).

[92] Identical letters dated 19 September 2024 from the Chargé d'affaires a.i. of the Permanent Mission of Lebanon to the UN addressed to the Secretary-General and the President of the Security Council (A/79/367–S/2024/685).

[93] Letter dated 16 June 2023 from the Permanent Representative of the Islamic Republic of Iran to the UN addressed to the Secretary-General and the President of the Security Council (S/2023/452).

[94] Identical letters dated 21 February 2020 from the Permanent Representative of Georgia to the UN addressed to the Secretary-General and the President of the Security Council (A/74/714–S/2020/135).

[95] Permanent Mission of Estonia to the UN (5 March 2020). "Joint press stakeout by Estonia, the United Kingdom and the United States on cyber-attack against Georgia".

[96] Reuters (20 February 2020). "Russia Rejects Allegations it Carried out Cyber Attack on Georgia – RIA".

discussion produced no formal outcome, it showed that Council members can use existing tools to highlight significant cyber-related concerns in a country-specific context, particularly where there is a risk of further escalation.

A more recent example occurred in September 2024, when the Council held a formal meeting on Lebanon under the agenda item "The situation in the Middle East, including the Palestinian question", following a Lebanese request for an emergency meeting and Algeria's push to place the matter before the Council. In its correspondence, Lebanon alleged that cyber operations had enabled the remote detonation of communication devices on 17 and 18 September 2024, resulting in civilian deaths, mass injuries, and severe strain on medical services.[97] Lebanon framed the incident as a violation of sovereignty and raised concerns under international humanitarian law in light of the scale of civilian harm and the method employed.

During the meeting, several Council members addressed the ICT-related dimension of the incident, emphasising that malicious activities involving ICTs may produce direct physical and humanitarian consequences.[98] The meeting, therefore, marked an instance of the Council considering, in a country-specific context, an incident described by a member state as cyber-related. Notably, Russia referred to confidence-building measures developed in the General Assembly's ICT processes and encouraged Lebanon to use the global intergovernmental Points of Contact Directory to clarify the circumstances and reduce the risk of escalation. This was particularly notable given Russia's broader reservations regarding the Council's role in addressing cyber-related issues.

Country-Specific Meetings related to Unmanned Aerial Systems

The Council has also addressed the use of unmanned aerial systems (UAS) in country-specific situations.[99] On 12 September 2025, it held an emergency briefing after Poland requested a meeting on reports that Russian drone-type objects had violated Polish airspace on the night of 9 and 10 September 2025.[100] The discussion focused on the implications of drone operations and airspace incursions for regional security and the risks of wider escalation, while Russia rejected the allegations as baseless.[101] The meeting highlighted the growing salience of unmanned and other technologically advanced systems in contemporary conflict.

The issue also arose at a 9 December 2025 briefing on Ukraine, where Tomaž Lovrenčič, Director of ITF Enhancing Human Security, described changes in modern warfare linked to the growing use of drones. He emphasised how these technologies were altering patterns of injury, civilian harm, and humanitarian need, illustrating how technological developments are reshaping conflict dynamics in situations before the Council.[102]

An earlier example came on 6 August 2021, when members discussed the 29 July 2021 attack on the oil tanker Mercer Street off the coast of Oman under "Any other business".[103] In a letter to the Council, Liberia, Romania, and the UK stated that initial assessments indicated it was "highly likely" that Iran had carried out the attack using one or more unmanned aerial vehicles and warned that such incidents posed risks to international peace and security.[104] Iran denied responsibility and described the accusation as unfounded.[105]

Security Council Thematic Products on Technology

The Council has adopted only one product on technology as a standalone thematic issue: a presidential statement on the impacts of scientific developments on peace and security.[106] Authored by Switzerland and adopted in October 2024, the statement affirms that scientific developments must be consistent with international law, including the purposes and principles of the UN Charter, and takes note of relevant General Assembly processes and resolutions. It also recognises that science, technology, and innovation can advance the work of the UN across its three pillars while noting that the convergence of scientific fields may accelerate technological capabilities in ways that carry both promise and risks for international peace and security and for the Council's work. The text further underscores the importance of international cooperation, capacity-building, and efforts to bridge scientific and technological divides, while expressing the Council's commitment to take scientific advances more systematically into account.

By contrast, the Council has not adopted a standalone thematic product on cybersecurity, despite efforts by some members to do so. Following the Council's first open debate on cybersecurity in June 2021, Estonia approached members on a bilateral basis to gauge interest in a draft presidential statement it had prepared. The draft text apparently expressed concern about the malicious use of ICTs and its implications for international peace and security, stressed the importance of promoting the peaceful use of ICTs and preventing conflict arising from their use, and emphasised the need for cooperation among states to reduce risks. It also underscored the importance of responsible state behaviour, noted that existing obligations under international law apply to states' ICT-related activity, and recognised the progress achieved through the General Assembly-led processes, particularly the cumulative consensus reports of the GGE and the OEWG.

Despite general support for the draft's objectives, Estonia's consultations revealed persistent divisions, including over language on the applicability of international law to state conduct in cyberspace and concerns that a Security Council product could pre-empt or interfere with parallel discussions in the General Assembly. Estonia, therefore, did not pursue the initiative further.

[97] Identical letters dated 19 September 2024 from the Chargé d'affaires a.i. of the Permanent Mission of Lebanon to the UN addressed to the Secretary-General and the President of the Security Council (A/79/367–S/2024/685).
[98] Security Council Meeting Record (20 September 2024) (S/PV.9730).
[99] The gender-neutral term "uncrewed" is sometimes used unofficially in place of "unmanned". However, "unmanned" remains the official term used by the UN in order to align with existing International Civil Aviation Organization (ICAO) terminology and regulations.
[100] Letter dated 10 September 2025 from the Permanent Representative of Poland to the UN addressed to the President of the Security Council (S/2025/572).
[101] Security Council Meeting Record (12 September 2025) (S/PV.9995).
[102] Security Council Meeting Record (9 December 2025) (S/PV.10057).
[103] Security Council Report. "Maritime Incident off the Coast of Oman: Meeting under "Any Other Business". What's in Blue. (5 August 2021): The meeting was requested by Estonia, France, Ireland, Norway, the UK, and the US.
[104] Letter dated 3 August 2021 from the representatives of Liberia, Romania and the United Kingdom of Great Britain and Northern Ireland to the UN addressed to the President of the Security Council (S/2021/701).
[105] Letter dated 4 August 2021 from the Chargé d'affaires a.i. of the Permanent Mission of the Islamic Republic of Iran to the UN addressed to the President of the Security Council (S/2021/706).
[106] Statement by the President of the Security Council (21 October 2024) (S/PRST/2024/6).

Overall, the limited number of standalone thematic Council products on technology reflects both Council practice and political dynamics. The Council has tended to approach new and politically sensitive issues incrementally, prioritising consensus-building in areas where mandates and institutional roles remain contested. Significant differences also persist among members regarding the appropriate scope of Council engagement on ICTs and new and emerging technologies, particularly where parallel processes are underway elsewhere in the UN system. These dynamics have constrained the Council's ability to translate thematic discussions into agreed outcomes and formal products.

International Law and Cyber Operations

Member states have repeatedly affirmed, including in successive consensus reports of the General Assembly-mandated GGE and OEWG processes, that existing international law, including the UN Charter, applies to state use of ICTs.[107] Significant differences remain, however, regarding how particular rules and thresholds operate in practice, including when cyber activity reaches relevant thresholds under jus ad bellum, when and how international humanitarian law applies to cyber operations, and whether the existing legal and normative framework is sufficient to address an evolving threat landscape. These differences are particularly evident among the permanent members of the Security Council, whose positions have shaped the Council's cautious approach to cyber-related issues and influenced the pace and character of its thematic engagement in this area.

The permanent members of the Security Council have affirmed in UN processes that existing international law, including the UN Charter, applies to state conduct in the use of ICTs.[108] This shared premise encompasses principles such as sovereign equality, non-intervention, the peaceful settlement of disputes, and the prohibition on the threat or use of force under Article 2(4). Within that common starting point, however, they continue to differ over how specific rules should be interpreted and applied in the cyber context.[109] These differences are especially evident in relation to jus ad bellum, including the circumstances in which cyber activities may constitute an armed attack for the purposes of Article 51, and the scope and conditions for the exercise of the inherent right of self-defence in response.

Divergent Views on "Use of Force" and "Armed Attack" in Cyberspace

In the absence of a treaty regime specifically addressing the use of force in cyberspace, the applicable framework remains grounded in the UN Charter and other rules of international law, including customary international law. As reflected in OEWG discussions, existing bodies of international law do not specifically address the use of ICTs in the context of international security, and international law may develop progressively, including through state practice and opinio juris.[110]

A number of states that have articulated views on jus ad bellum in cyberspace, including France, the UK, and the US, consider that cyber operations may, in certain circumstances, constitute a "use of force" under Article 2(4), particularly where their scale and effects are comparable to those of conventional military action. In this view, the assessment focuses on consequences rather than the means employed.[111] Cyber operations resulting in death, injury, or significant physical destruction are frequently cited as examples that could meet this threshold, including operations that trigger a nuclear plant meltdown, breach a dam and cause flooding above a populated area, or disable air traffic control systems in ways that could lead to aircraft crashes.[112]

Differences among the permanent members are more pronounced with respect to Article 51. That provision recognises the inherent right of individual or collective self-defence if "an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security". The 2014-2015 GGE recognised the "inherent right of States to take measures consistent with international law and as recognized in the Charter", while also noting the "need for further study" on the matter.[113]

Among the permanent members, France, the UK and the US have affirmed that cyber operations may, depending on their scale and effects, constitute an "armed attack" giving rise to the inherent right of self-defence, while differing on the circumstances in which self-defence may be invoked in response to cyber activities by non-state actors.[114]

[107] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (22 July 2015) (A/70/174); Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (18 March 2021) (A/75/816); and Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (14 July 2021) (A/76/135).

[108] Official Compendium of Voluntary National Contributions on the subject of how International Law applies to the Use of Information and Communications Technologies by States (13 July 2021) (A/76/136). See, for example, Russia's contribution: "Russia assumes that, for the present, the international community has reached consensus on the applicability of the universally accepted principles and norms of international law, which are enshrined, first and foremost, in the Charter of the United Nations". See also Statement by China on the Application of International Law at the first meeting of the UN OEWG on security of and in the use of ICTs 2021–2025 (16 December 2021): "China agrees that the general principles of international law based on the UN Charter apply to cyberspace".

[109] Russia, for example, has stated that, while it assumes that the international community has reached consensus on the applicability to the information space of the universally accepted principles and norms of international law, as enshrined in the UN Charter, the application of international law to the use of ICTs "should not be automatic" and should not "be carried out by simple extrapolation". It has argued that the "unique technical and legal features" of the information environment – such as the cross-border and pervasive nature of ICTs, the anonymity of their use and attribution challenges – preclude the automatic and full application of existing international law norms.

[110] Chair's Summary, Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (10 March 2021) (A/AC.290/2021/CRP.3): "while existing bodies of international law do not include specific reference to the use of ICTs in the context of international security, international law can develop progressively, including through opinio juris and State practice"; noting that "the possibility over time of developing complementary binding measures concurrently with the implementation of norms was raised" and that "a political commitment was proposed as one possible way forward".

[111] Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of ICTs by States (13 July 2021) (A/76/136). See, for example, the UK's voluntary national contribution, which notes that "conduct by States carried out in cyberspace is capable of constituting a threat or use of force if the actual or threatened conduct has or would have the same or similar effects of conduct using kinetic means"; and the US' contribution, which states that "if the physical consequences of a cyber activity result in the kind of damage that dropping a bomb or firing a missile would, that cyber activity should equally be considered a use of force [or] armed attack". See also France's working paper, entitled "International law applied to operations in cyberspace", submitted to the OEWG, which notes that "a cyberoperation carried out by one State against another State violates the prohibition of the use of force if its effects are similar to those that result from the use of conventional weapons".

[112] See, for example, Harold Hongju Koh, Legal Adviser, U.S. Department of State (September 18, 2012). "Remarks at the USCYBERCOM Inter-Agency Legal Conference", Fort Meade, MD.

[113] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (22 July 2015) (A/70/174).

[114] Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of ICTs by States (13 July 2021) (A/76/136). See, for example,

By contrast, China has argued that consideration of the applicability of jus ad bellum should be "handled with prudence".[115] While affirming that the general principles of international law based on the Charter apply to cyberspace, it has emphasised that discussions on the applicability of existing international law should "adhere to the overarching goal of maintaining peace in cyberspace and always be premised on 'not encouraging or legitimising conflict'".[116] Russia has similarly recognised consensus on the applicability of the universally accepted principles and norms of international law, as enshrined in the UN Charter, while emphasising what it sees as a lack of consensus on the issue of "qualifying malicious use of ICTs as an 'armed attack' in the sense of Article 51".[117]

These divergent interpretations intersect with broader disagreements over whether existing international law, complemented by the voluntary, non-binding norms, is sufficient to address state use of ICTs.[118] Some states consider the existing legal and normative framework adequate and emphasise the importance of implementing agreed norms of responsible state behaviour, alongside confidence-building and capacity-building measures. Others, including China and Russia, have called for the development of new legally binding instruments tailored to ICTs.[119] In March 2023, Russia submitted to the OEWG an updated concept note setting out elements of a proposed UN convention on international information security, including arrangements for implementation, exchanges on implementation, peaceful settlement of disputes, and a verification mechanism operating under UN auspices.[120]

Section IV: Mapping Technology Issues Across Security Council Agenda Items

Although the Security Council's engagement on ICTs, AI, and new and emerging technologies as standalone thematic issues is relatively recent, the peace and security implications of these technologies have intersected with its work for much longer, particularly through its thematic agenda items. This overlap has become more pronounced as new technologies play an increasingly important role in contemporary conflict dynamics.

Across multiple agenda items, Council members have increasingly referred to cyber operations targeting critical infrastructure, the exploitation of online spaces for terrorist purposes, the use of new technologies to facilitate sanctions evasion and other forms of illicit finance, and the role of online information manipulation in the deterioration of protection environments. The Council has also considered the operational use of technology in counter-terrorism, the protection of civilians, and peace operations.

This section maps selected points of intersection between technology and the Council's thematic agenda items, identifying recurrent pathways through which technological issues surface in deliberations and products. In doing so, it highlights areas where the Council has developed a more consistent vocabulary and set of concerns related to technology, as well as areas where engagement remains fragmented, episodic, or contested.

Technology and Counter-terrorism

Terrorists and terrorist groups have long exploited ICTs not only to carry out attacks, but also to support a wide range of related activities, including incitement, radicalisation, recruitment, training, planning, communications, operational preparation, procurement, and financing. As reflected in national strategies and UN counter-terrorism discussions, many states now treat terrorist exploitation of the Internet and related digital tools as both a national and an international security concern.[121]

The Council has engaged more consistently with technology in the context of counter-terrorism than under any other agenda item. Over time, it has increasingly addressed the use of ICTs and new and emerging technologies for terrorist purposes through a substantial body of resolutions and related policy work. Much of this engagement has been operationalised at the subsidiary level, notably through the Counter-Terrorism Committee (CTC) and its Executive Directorate (CTED), which support implementation through

the voluntary national contributions of the UK, noting that "an operation carried out by cyber means may constitute an armed attack giving rise to the inherent right of individual or collective self-defence, as recognised in Article 51 of the UN Charter where the scale and effects of the operation are equivalent to those of an armed attack using kinetic means"; and the US, stating that "a State's inherent right of self-defense, recognized in Article 51 of the UN Charter, may in certain circumstances be triggered by cyber activities that amount to an actual or imminent armed attack. This inherent right of self-defense against an actual or imminent armed attack in or through cyberspace applies whether the attacker is a State actor or a non-State actor". See also France (2021), "International Law Applied to Operations in Cyberspace", paper shared with the OEWG, noting that "a cyberattack may constitute an armed attack within the meaning of Article 51 of the United Nations Charter, if it is of a scale and severity comparable to those resulting from the use of physical force", and adding that "[t]o be categorised as an armed attack, a cyberattack must also have been perpetrated, directly or indirectly, by a State".

[115] China's Submissions to the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (September 2019).

[116] Statement by China on the Application of International Law at the first meeting of the UN Open-ended Working Group on security of and in the use of ICTs 2021–2025 (16 December 2021).

[117] Official Compendium of Voluntary National Contributions on the subject of how International Law applies to the Use of Information and Communications Technologies by States (13 July 2021) (A/76/136); See also Permanent Mission of the Russian Federation to the UN (7 March 2023). "Statement by its representative at the fourth substantive session of the UN Open-ended Working Group on Security of and in the Use of ICTs 2021–2025", New York, NY.

[118] See the Chair's Summary of the third substantive session of the OEWG on Developments in the Field of ICTs in the Context of International Security (8-12 March 2021) (A/AC.290/2021/CRP.3).

[119] Statement by China on the Application of International Law at the first meeting of the UN Open-ended Working Group on security of and in the use of ICTs 2021–2025 (16 December 2021); See also: Russia argued that the draft final report of the OEWG 2021-2025 contained "an unjustified bias in favour of only implementing the existing list of voluntary norms", noting that the "importance of giving voluntary, non-binding rules of behaviour a legally binding status [was] missing". (7 July 2025).

[120] Updated Concept of the Convention of the United Nations on Ensuring International Information Security, submitted by the Russian Federation to the OEWG (7 March 2023), section VI.

[121] Camino Kavanagh (2017). The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century, Geneva, Switzerland: UNIDIR.

country assessments, the facilitation of technical assistance, and the development of analytical and guidance products.[122]

Within this framework, technology is often treated in functional terms, both as an enabler of terrorist activity and as part of the state response. The latter includes the collection and use of digital and biometric data, the handling of electronic evidence in the investigation and prosecution of terrorism-related offences, and efforts to protect critical infrastructure and essential services from attacks conducted in or through cyberspace.[123]

While Council dynamics have constrained efforts to address ICTs as a standalone thematic issue, the security dimensions of these technologies have nonetheless been progressively integrated into the Council's counter-terrorism framework. In practice, this integration has developed along several distinct, though interrelated, strands.

The Use of ICTs for Terrorist Purposes

One strand of the Security Council's counter-terrorism framework concerns the use of ICTs to facilitate terrorist activity. Resolution 1373 (2001), adopted shortly after the attacks of 11 September 2001 and establishing the CTC, called on member states to intensify and accelerate the exchange of operational information, including on the "use of communication technologies by terrorist groups".[124]

Over time, the Council's counter-terrorism framework has increasingly recognised the role of ICTs, in particular the Internet, in enabling a wider range of terrorist activity. Resolution 2129 (2013) noted the evolving nexus between terrorism and ICTs and their use to commit or facilitate terrorist acts, including through incitement, recruitment, financing, and planning. Resolution 2250 (2015), which focused on youth, peace and security, expressed concern about the increased use of ICTs, in particular the Internet, by terrorists and their supporters for the recruitment and incitement of youth. Resolution 2354 (2017), in turn, noted with concern the use of terrorist narratives to recruit supporters and foreign terrorist fighters, mobilise resources, and garner support from sympathisers, including through the exploitation of ICTs, the Internet, and social media.[125]

The Council has also increasingly articulated expectations for states to take action. Resolution 1624 (2005) called for "necessary and appropriate measures", consistent with international law, to prohibit and prevent incitement to commit terrorist acts. As concerns grew about the exploitation of the Internet and other communications technologies for radicalisation and incitement, resolution 2178 (2014) urged cooperative action to prevent terrorists, in particular foreign terrorist fighters, from exploiting technology, communications, and resources to incite support for terrorist activity.[126] Resolution 2354 complemented these measures by endorsing a Comprehensive International Framework to Counter-Terrorist Narratives, while the CTC further elaborated related guidance through the 2015 Madrid Guiding Principles[127] and the 2018 Addendum,[128] including on approaches to monitoring and analysing terrorist content transmitted via the Internet and other ICTs.

The Council has also recognised the importance of digital technologies to law enforcement, border security, and accountability. Several resolutions call on member states to strengthen cooperation in the investigation and prosecution of terrorism-related offences, including through the collection, handling, preservation, and sharing of relevant information and evidence.[129] Resolution 2396 (2017), for example, advanced measures related to the use of biometric data to identify terrorists, while also encouraging member state cooperation with the private sector, including ICT companies, in gathering digital data and evidence in cases related to terrorism and foreign terrorist fighters.

In support of these priorities, CTED, the International Association of Prosecutors, and the UN Office on Drugs and Crime launched a global initiative to strengthen the capacity of investigators and prosecutors to preserve and obtain electronic evidence in cross-border cases and to enhance cooperation with the private sector.[130] In addition, Tech Against Terrorism was launched in 2017 by CTED and Swiss NGO ICT4Peace as an initiative to promote responsible industry approaches to addressing terrorist use of the Internet while respecting human rights and fundamental freedoms.[131]

Terrorist Cyberattacks on Critical Infrastructure

A second strand, which the Security Council and the CTC have addressed together, is the protection of critical infrastructure from terrorist attacks, including those conducted in or through cyberspace. The CTC held open briefings on this issue in June 2014 and June 2015, and Ukraine later convened an Arria-formula meeting on 21 November 2016 on the protection of critical infrastructure against terrorist attacks.[132] The concept note for that meeting underscored that attacks against critical infrastructure, whether physical or cyber in nature, could severely undermine the stability of affected societies. In February 2017, under Ukraine's presidency, the Council returned to the issue in an open debate focused on both physical and emerging threats to infrastructure, including those involving ICTs.[133]

[122] UN Security Council Counter-Terrorism Committee (CTC). "Facilitation of Technical Assistance"; Counter-Terrorism Committee Executive Directorate (CTED). "Trends Alert" series.

[123] CTED. "CTED input to the OEWG ICT Mapping Exercise": paper prepared in response to the UNODA letter (ODA/2023-00042/ICT-Mapping Exercise) (2023).

[124] Security Council Resolution 1373 (28 September 2001) (S/RES/1373).

[125] Resolution 2354 (2017) built on the Council's presidential statement of May 2016 (S/PRST/2016/6), which requested the CTC develop a proposal for a "comprehensive international framework" to counter the narratives used by ISIL, Al-Qaida, and associated entities to encourage, motivate, and recruit individuals to commit terrorist acts.

[126] Security Council Resolution 2178 (24 September 2014) (S/RES/2178).

[127] Letter dated 15 December 2015 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism addressed to the President of the Security Council (S/2015/939).

[128] Letter dated 28 December 2018 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism addressed to the President of the Security Council (S/2018/1177).

[129] Security Council Resolution 2322 (12 December 2016) (S/RES/2322); Security Council Resolution 2396 (21 December 2017) (S/RES/2396); and Security Council Resolution 2331 (20 December 2016) (S/RES/2331).

[130] UNODC (1 February 2019). "UNODC and partners release Practical Guide for Requesting Electronic Evidence Across Borders"; UN Security Council CTC. "2019 Activities of the CTED/UNODC/IAP Global Initiative on digital evidence across borders".

[131] CTED. "Launch of 'Tech Against Terrorism' – a partnership between technology companies, governments, and UN CTED" (19 April 2017); Security Council Resolution 2396 (21 December 2017) (S/RES/2396).

[132] CTED, INTERPOL, and UN Office of Counter-Terrorism (UNOCT) (2018). Compendium of Good Practices on the Protection of Critical Infrastructure against Terrorist Attacks; See also Security Council Report. "Open Arria-formula Meeting on Counter-terrorism". What's in Blue. (21 November 2016); Permanent Mission of Ukraine to the UN (23 November 2016). "Ukraine initiated the UN Security Council Arria-formula meeting on the protection of critical infrastructure against terrorist attacks".

[133] Security Council Meeting Record (13 February 2017) (S/PV.7882): Council debate on "Protection of critical infrastructure against terrorist attacks"; Security Council Report. "Open Debate and Draft Resolution on Protection of Critical Infrastructure against Terrorist Attacks". What's in Blue. (11 February 2017).

At that meeting, the Council adopted resolution 2341 (2017), which remains the only Security Council resolution to date to refer expressly to "cybersecurity".[134] The resolution recognised that protecting critical infrastructure from terrorist attacks requires multiple, complementary lines of effort, including cybersecurity, and called on member states to strengthen risk-reduction strategies and preparedness and response capacities. It also directed the CTC, with the support of CTED, to examine member states' efforts to protect critical infrastructure from terrorist attacks with a view to identifying good practices, gaps, and vulnerabilities. In support of that work, CTED, INTERPOL, and the UN Office of Counter-Terrorism (UNOCT) jointly published a compendium of good practices in 2018, with an updated edition issued in 2022.[135]

More recently, CTED has increasingly integrated cyber-related vulnerabilities into its broader assessment of terrorist threats to critical infrastructure. A November 2025 trend report update issued jointly by CTED and the Organization for Security and Co-operation in Europe (OSCE) highlighted the growing integration of digital technologies into critical infrastructure operations and the resulting interconnection between cyber and physical security risks.[136] As a larger share of these systems becomes networked or connected to the Internet, the report notes that they are increasingly exposed to cyberattacks capable of producing significant physical consequences.

The report also noted that, while new technologies, including AI, can improve operational efficiency, support predictive maintenance, and strengthen emergency responses related to critical infrastructure, they may also create new opportunities for malicious actors to disrupt or damage its functioning. It further observed that, although many states have begun addressing threats to critical infrastructure posed by ICTs and new technologies, including through ICT- and AI-specific legislation and national cybersecurity strategies, others have yet to do so, either because of limited capacity or the difficulty of putting in place legislative frameworks in this area.

The Use of New and Emerging Technologies for Terrorist Purposes

A third strand of the Security Council's counter-terrorism engagement concerns the use of new and emerging technologies by terrorist actors, extending beyond the more familiar facilitative role associated with ICTs.[137] In recent years, the Council, particularly through the CTC, and CTED have increasingly examined how terrorists may exploit unmanned aircraft systems (UAS), new and emerging financial technologies, AI, and other dual-use technologies.[138] This reflects concern that rapid technological change may expand terrorists' operational capabilities, lower barriers to entry, and complicate prevention, detection, and accountability.

At the normative level, this work builds on the Council's earlier recognition that terrorists adapt to and exploit technological change. While initial attention centred on ICTs, subsequent Council products have provided a broader basis for examining emerging and future risks. Resolution 2617 (2021), which renewed CTED's mandate, referred not only to terrorist use of ICTs but also to "other emerging technologies". At the same time, the Council has advanced this agenda primarily through subsidiary-body processes, thematic discussions, and non-binding guidance, rather than through new binding obligations.

This approach crystallised during India's chairmanship of the CTC in 2022, when the Committee convened a special meeting in Mumbai and New Delhi on 28 and 29 October 2022 on countering the use of new and emerging technologies for terrorist purposes. Discussions focused on three interrelated areas: terrorist misuse of UAS; risks and opportunities associated with new payment technologies and digital fundraising methods; and the broader technological ecosystem, including ICTs. The meeting underscored that many emerging technologies are dual-use and widely accessible for legitimate civilian and commercial purposes, while stressing the need to balance innovation with efforts to prevent and counter terrorist misuse.[139]

The special meeting concluded with the adoption of the Delhi Declaration. While non-binding, the Declaration reflected a shared understanding among CTC members of the risks posed by emerging technologies. It reaffirmed that terrorism in all forms and manifestations remains one of the most serious threats to international peace and security, noted with concern the increased use by terrorists of the Internet and other ICTs, including social media platforms, and highlighted the growing misuse of UAS to conduct attacks against critical infrastructure and public places and to facilitate illicit trafficking.[140] It also expressed the CTC's intention, with CTED's support, to develop non-binding guiding principles on the meeting's principal themes.[141]

Follow-up to the Delhi Declaration has taken place mainly at the subsidiary level. In December 2023, the CTC adopted the Abu Dhabi Guiding Principles on the threats posed by the use of UAS for terrorist purposes. These provide non-binding guidance on integrating UAS threats into national counter-terrorism strategies and legal frameworks, improving awareness of UAS-related risks, developing measures to detect and respond to such threats, and strengthening capacity development and information exchange.[142] This work built on earlier Council recognition of the issue, including resolution 2370 (2017), which condemned the continued flow of weapons, including UAS and their components, to terrorist groups, and resolution 2617, which noted with concern the growing global misuse of UAS by terrorists to conduct attacks against restricted commercial and government infrastructure and public places.

A second set of non-binding guidance—the Algeria Guiding Principles—was adopted in January 2025 and addresses terrorist

[134] Security Council Resolution 2341 (13 February 2017) (S/RES/2341).

[135] CTED, INTERPOL, and UNOCT (2018). Compendium of Good Practices on the Protection of Critical Infrastructure against Terrorist Attacks; CTED, INTERPOL, and UNOCT (2022). Compendium of Good Practices 2022 Update: The Protection of Critical Infrastructure against Terrorist Attacks.

[136] CTED and Organization for Security and Co-operation in Europe (OSCE) (November 2025). Trends Report Update: Physical Protection of Critical Infrastructure Against Terrorist Attacks.

[137] UN Security Council CTC. "Countering the Use of New and Emerging Technologies for Terrorist Purposes".

[138] See, for example, CTED. CTED Trends Alert (May 2019): Greater Efforts Needed to Address the Potential Risks Posed by Terrorist Use of Unmanned Aircraft Systems (UAS).

[139] CTED. "Information and Communication Technologies (ICT) and Emerging Technologies".

[140] Security Council CTC: Delhi Declaration on Countering the Use of New and Emerging Technologies for Terrorist Purposes (29 October 2022) (S/2022/998).

[141] Ibid., para. 30.

[142] Letter dated 19 December 2023 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism, addressed to the President of the Security Council, transmitting the Committee's non-binding guiding principles on threats posed by the use of unmanned aircraft systems for terrorist purposes ("Abu Dhabi Guiding Principles") (26 December 2023) (S/2023/1035); United Arab Emirates Ministry of Foreign Affairs (31 December 2023). "The Security Council Counter-Terrorism Committee Adopts the Abu Dhabi Guiding Principles on the Threats Posed by the Use of Unmanned Aircraft Systems for Terrorist Purposes".

use of new and emerging financial technologies, including virtual assets, online payment systems, and digital fundraising tools. Building on existing counter-terrorist financing frameworks, the principles emphasise a comprehensive, risk-based approach to vulnerabilities associated with financial innovation while recognising the legitimate benefits of such technologies.[143] They also stress the need to strengthen national measures and international cooperation to prevent, detect, and disrupt such misuse.[144]

Although the Delhi Declaration also identified ICTs as a core area for follow-up, the Committee had not, as of March 2026, adopted a corresponding third set of non-binding guiding principles focused specifically on terrorist exploitation of ICTs and the Internet. The delay may partly reflect the broader political and regulatory sensitivity of ICT-related issues, as well as the relative absence of comparably well-developed international standard-setting and regulatory frameworks.[145]

CTED has also continued to track new trends and evolving threats in terrorist use of ICTs and emerging technologies, including advances in AI and machine learning, generative AI and deepfakes, algorithmic curation and amplification processes that can facilitate the spread of harmful and violent content, gaming platforms and related online spaces such as augmented reality and virtual reality platforms, and other dual-use technologies that may broaden terrorists' reach or capabilities such as 3D printing, self-driving cars, and advanced robotics.[146]

Beyond the work of the CTC and CTED, other Council subsidiary bodies have also examined the implications of technological change for terrorist activity within their respective mandates. In particular, the 1540 Committee has addressed risks associated with scientific and technological advances in the context of preventing non-state actors from acquiring weapons of mass destruction and their means of delivery. Resolution 2663 (2022), which extended the mandate of the 1540 Committee and its Group of Experts, expressed grave concern that non-state actors might acquire, develop, traffic in, or use nuclear, chemical, or biological weapons, including through the exploitation of advances in science, technology, and international commerce. While grounded in a non-proliferation framework, this practice illustrates the broader integration of technology considerations across the Council's subsidiary architecture.

Technology and the Protection of Civilians

The Security Council has increasingly acknowledged the nexus between the protection of civilians in armed conflict (PoC) and developments in ICTs and new technologies. Member states and the Secretary-General have drawn attention to the ways in which cyber operations, AI, autonomous weapons systems, and related technologies may have direct and indirect implications for civilian protection.

These concerns have also been raised in other multilateral fora. The final report of the 2021–2025 OEWG, for example, noted that states are developing ICT capabilities for military purposes and that the such capabilities have already been used in conflicts in different regions, affecting civilians and civilian objects.[147] Related concerns were also apparent at the 34th International Conference of the Red Cross and Red Crescent, held in Geneva from 28 to 31 October 2024, where states adopted a resolution on "Protecting civilians and other protected persons and objects against the potential human cost of ICT activities during armed conflict".[148] The resolution expressed concern that malicious ICT activities by parties to armed conflict may harm civilians and other protected persons and objects, including civilian critical infrastructure, and reiterated that, in situations of armed conflict, international humanitarian law (IHL) rules and principles protect civilians and other protected persons and objects against the risks arising from such activities, while recognising that the specificities of the ICT environment continue to raise questions about how those rules and principles apply in practice.[149]

The Secretary-General's 2025 annual report on PoC brought these issues into sharper focus within the Council's own protection framework. For the first time, it included a dedicated section on "new technologies, trends in compliance and working towards the full protection of civilians". The report underscored that, because ICT activities can damage critical infrastructure, disrupt essential services, and delete vital data, even without causing physical damage, their use in armed conflict raises concerns regarding compliance with IHL and the protection of civilians. It further observed that ICT use can draw civilians into hostilities more readily, increasing their exposure to direct or incidental harm. Moreover, it suggested that, while there is growing recognition that ICT activities during armed conflict are governed by IHL, it remains critical to arrive at a common understanding of how IHL rules apply in practice and to ensure awareness of the risks associated with civilian involvement.

The Applicability of International Humanitarian Law to ICT Activities

As military cyber capabilities proliferate, questions about how and when IHL applies to cyber operations have become increasingly pertinent. Successive UN processes clarified some baseline parameters while leaving important questions unresolved. The 2014–2015 GGE noted established international legal principles, including humanity, necessity, proportionality, and distinction, in the context of the use of ICTs by states, while the 2019–2021 GGE recognised the need for further study on how and when those principles apply.[150]

[143] In resolution 2462 (2019), the Security Council noted that terrorists may move and transfer funds through "emerging payment methods" such as prepaid cards, mobile payments, and virtual assets. It also highlighted potential risks associated with virtual assets and new financial instruments, including crowdfunding platforms, that may be "abused for the purpose of terrorist financing". In resolution 2617 (2021), the Council recognised that "innovations in financial technologies, products and services may offer significant economic opportunities but also present a risk of being misused, including for terrorist financing".

[144] Technical Guide to the Implementation of Security Council Resolution 1373 (2001) and Other Relevant Resolutions (18 August 2017) (S/2017/716).

[145] For example, work on UAS and emerging financial technologies has benefited from the existence of comparatively well-developed international standard-setting and regulatory frameworks. See, for example, International Civil Aviation Organisation (ICAO), Unmanned Aircraft Systems (UAS) Circular 328–AN/190 (2011); and Financial Action Task Force (FATF), Comprehensive Update on Terrorist Financing Risks (July 2025).

[146] CTED. "Information and Communication Technologies (ICT) and Emerging Technologies".

[147] Final Report of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025 (24 July 2025) (A/80/257).

[148] Resolution 2 of the 34th International Conference of the Red Cross and Red Crescent. "Protecting civilians and other protected persons and objects against the potential human cost of ICT activities during armed conflict" (October 2024) (34IC/24/R2).

[149] The resolution also recognised that an increasingly digitalised and interconnected world can save and improve lives, including in armed conflict, and underscored the importance of connectivity and ICTs for the delivery of medical services, humanitarian operations, access to information needed for safety and survival, and the maintenance or restoration of family links.

[150] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (22 July 2015) (A/70/174); Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (14 July 2021) (A/76/135).

Applying IHL in practice presents distinct challenges in the cyber context. Many civilian and military networks are interconnected, and military networks may rely on civilian cyber infrastructure, complicating the identification of civilian objects protected under IHL and the assessment of incidental civilian harm.[151] Cyber operations may also generate indirect or cascading effects across shared networks, potentially disrupting essential services beyond the immediate target. In addition, while cyber operations targeting essential civilian data could cause serious harm to civilians, whether, and to what extent, data constitutes an "object" for the purposes of the rules on attacks under IHL continues to be debated.[152]

Nevertheless, in situations of international and non-international armed conflict, there is growing recognition that IHL applies to cyber operations carried out in the context of hostilities, including when such operations are conducted alongside, or in support of, kinetic military action.[153] Proponents of this view have often invoked the International Court of Justice's Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons, in which the Court observed that the "intrinsically humanitarian character" of the established principles and rules of IHL "permeates the entire law of armed conflict and applies to all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future".[154]

These questions have exposed significant differences among the Council's permanent members. The UK and the US have stated that cyber activities in the context of armed conflict may, in certain circumstances, constitute an "attack" for the purpose of applying IHL, and that where a cyber operation amounts to an "attack", the relevant IHL principles and rules apply irrespective of the operational domain.[155] France has similarly stated that IHL applies to cyber operations carried out in, and in connection with, armed conflict, and has set out its views on when a cyber operation may constitute an attack within the meaning of IHL.[156]

Russia, by contrast, has stated that, in the absence of what it considers consensus in the international community on qualifying the malicious use of ICTs as an "armed attack" in the sense of Article 51 of the UN Charter, "there are no grounds for assessing the legality of the use of ICTs from the IHL perspective".[157] China has similarly stated that "the applicability of the law of armed conflicts and jus ad bellum needs to be handled with prudence" and that "the lawfulness of cyber war should not be recognized under any circumstance".[158]

Some states, in turn, have sought to address concerns that recognising the applicability of IHL to ICT activities in armed conflict could be seen as legitimising conflict in cyberspace. The resolution adopted at the 34th International Conference of the Red Cross and Red Crescent emphasised that recalling IHL in relation to ICT activities "by no means legitimizes or encourages conflict", while also recognising both the diversity of state views and the need for continued discussion on how IHL principles apply.[159] These differences resurfaced during negotiations on the final report of the OEWG in July 2025. Russia opposed any mention of the resolution, which it described as "non-consensual", citing the central role of the UN, and in particular the OEWG, in discussions on the applicability of international law to the use of ICTs.[160] France, by contrast, argued that the resolution represented an "important and consensual step forward" that had been referred to within the OEWG on numerous occasions, while welcoming the continuation of this work through the ICRC's Global Initiative.[161]

Cyberattacks against Critical Infrastructure and the Protection of Civilians

The protection of critical civilian infrastructure has emerged as an important concern within the PoC framework. There is no universally agreed definition of "critical infrastructure". As the final report of the 2021-2025 OEWG noted, it remains the sovereign prerogative of each state to determine which infrastructures it designated as critical.[162] In Security Council discussions, however, the term has generally been used to refer to civilian infrastructure and services whose disruption or destruction could have deleterious effects for the population, including energy systems, health-care services, water and sanitation, transportation networks, and communications infrastructure. Council members have underscored that cyber operations targeting such sectors may carry significant humanitarian consequences, particularly given the growing digitisation of essential services and the potential for cascading effects, including across borders. Some have also highlighted the risks posed to nuclear facilities and other high-risk installations.

In Council meetings, some member states have argued that the PoC agenda should more explicitly encompass the risks posed by

[151] International Committee of the Red Cross (ICRC) Position Paper on International Humanitarian Law and Cyber Operations during Armed Conflicts (28 November 2019).

[152] Ibid.

[153] Open-ended Working Group on Security of and in the Use of Information and Communications Technologies (9 July 2025). "Working Paper on the Application of International Humanitarian Law to the Use of Information and Communication Technologies in Situations of Armed Conflict", submitted by Brazil, Canada, Chile, Colombia, the Czech Republic, Estonia, Germany, the Netherlands, Mexico, the Republic of Korea, Senegal, Sweden and Switzerland.

[154] Advisory Opinion of the International Court of Justice (ICJ) on the Legality of the Threat or Use of Nuclear Weapons (1996), ICJ Reports, page 226, para. 86.

[155] Official Compendium of Voluntary National Contributions on the subject of how International Law applies to the Use of Information and Communications Technologies by States (13 July 2021) (A/76/136).

[156] France has stated that IHL applies to "all cyberoperations carried out in, and in connection with, an armed conflict situation", including operations that do not amount to an "attack" within the meaning of IHL. It has further stated that "most cyberoperations carried out by the French armed forces in an armed conflict situation (mainly information-gathering) do not meet the definition of an attack", but "are still governed by the provisions of IHL applicable to any military operation carried out in an armed conflict situation". France also considers that a cyberoperation may qualify as an attack where "the targeted equipment or systems no longer provide the service for which they were implemented, whether temporarily or permanently, reversibly or not", including where, if the effects are temporary or reversible, "action by the adversary is necessary to restore the infrastructure or system". France (2021). "International law Applied to Operations in Cyberspace", paper shared with the Open-ended Working Group established by General Assembly resolution 75/240 (2020).

[157] Statement by the Representative of the Russian Federation at the Fourth Session of the UN Open-Ended Working Group on Security of and in the Use of ICTs 2021–2025, New York, NY (7 March 2023).

[158] China's Submissions to the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (September 2019).

[159] Resolution 2 of the 34th International Conference of the Red Cross and Red Crescent. "Protecting civilians and other protected persons and objects against the potential human cost of ICT activities during armed conflict" (October 2024) (34IC/24/R2).

[160] Statement by the Russian Interagency Delegation at the Eleventh Session of the UN Open-Ended Working Group on Security of and in the Use of ICTs 2021–2025, New York, NY (7 July 2025).

[161] Open-ended Working Group (OEWG) 2021–2025 on Security of and in the Use of Information and Communications Technologies, 11th Substantive Session, New York, NY (7–11 July 2025): Projets d'intervention de la délégation française.

[162] Final Report of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025 (24 July 2025) (A/80/257).

cyber activities and other technologies to civilian populations during armed conflict, particularly where attacks on critical infrastructure or disruptions to essential services may have cascading effects on civilians.[163] On 27 April 2021, the Council held an open debate on "Critical Infrastructure: The Protection of Objects Indispensable to the Survival of the Civilian Population" under the PoC agenda item and adopted resolution 2573 (2021). Although the resolution did not explicitly refer to cyber operations, several members warned during the debate that cyberattacks against electricity, water, and healthcare systems, particularly in urban settings, could deprive large numbers of civilians of essential services and undermine humanitarian action.[164] Similar concerns later appeared in the June 2021 and June 2024 open debates on cyber threats, as well as in the November 2024 briefing on "threats posed by ransomware attacks against hospitals and other healthcare facilities and services".[165]

Arria-formula meetings have provided additional space for more focused discussion. On 26 August 2020, Indonesia, in cooperation with Belgium, Estonia, Viet Nam, and the ICRC, convened an Arria-formula meeting on "Cyber-Attacks Against Critical Infrastructure".[166] On 25 May 2023, Albania and the US, with co-sponsorship by Ecuador and Estonia, organised an Arria-formula meeting on "The Responsibility and Responsiveness of States to Cyberattacks on Critical Infrastructure".[167] Together, these discussions pointed to broad convergence around the need to protect critical infrastructure from malicious ICT activity, with several member states describing cyberattacks against critical infrastructure and critical information infrastructure as a growing threat to international peace and security. Council members also frequently pointed to the normative framework of responsible state behaviour in cyberspace as central to these efforts.[168]

These discussions have unfolded alongside broader reflections on the evolution of the PoC agenda. Since the Security Council added the protection of civilians in armed conflict to its agenda in 1999, its engagement on PoC has expanded to address a wide range of specific threats to civilians. The growing prominence of technology-related risks in PoC debates and the Secretary-General's reports form part of that broader adaptation of the agenda to contemporary conflict dynamics. At the same time, concerns have periodically been raised that the proliferation of sub-themes could fragment the PoC agenda and detract from a holistic focus on compliance with IHL.[169]

Among the permanent members, France, the UK, and the US have generally favoured a more expansive and operational approach to PoC, while China and Russia have placed greater emphasis on state sovereignty, limits on mandate interpretation, and the risk of politicisation. As a result, PoC debates have at times mirrored broader geopolitical divisions, even as a basic consensus on the importance of civilian protection, particularly in peacekeeping settings, has remained.[170] These tensions have become more pronounced where PoC concerns intersect with ICT activities and new technologies in conflict. In that context, questions of legal applicability, attribution, and state responsibility have drawn greater attention, alongside broader sensitivities about mandate expansion and possible fragmentation of the PoC agenda.

Online Misinformation, Disinformation, and Hate Speech

The manipulation of online information has become a significant concern for the protection of civilians, particularly because ICTs can amplify the scale, speed, and reach of harmful narratives. The final report of the 2021-2025 OEWG noted states' concern about the malicious use of ICT-enabled covert information campaigns to influence the processes, systems, and overall stability of other states, including those in transitional phases or emerging from armed conflict.[171] It further noted that such activity could erode trust, prove escalatory, and threaten international peace and security, while also causing direct and indirect harm to individuals. The report also raised concern about malicious ICT activity targeting international and humanitarian organisations, including UN missions, which could undermine trust in their work and disrupt their ability to carry out their mandates in a safe, secure, and independent manner.

Recent reports of the Secretary-General on PoC have echoed these concerns, underscoring that the malicious use of ICTs could "polarize attitudes, fuel violence, distort facts on which people rely to make decisions for safety, and undermine trust in and acceptance of humanitarian activities".[172] They have also pointed to concrete examples across several contexts. In Sudan, harmful information on social media reportedly exacerbated divisions and fuelled violence, including the killing of dozens of people.[173] In Burkina Faso, misinformation and disinformation discrediting humanitarian actors undermined trust, created security risks, and hindered efforts to

[163] Security Council Meeting Record (20 June 2024) (S/PV.9662). See, for example, Statement by Costa Rica, emphasising that the protection of civilians' agenda should be extended to encompass cyber-activities affecting civilian populations during armed conflicts.

[164] During the open debate on 27 April 2021, several Council members drew attention to the humanitarian risks posed by cyber operations targeting critical civilian infrastructure. Ireland, for example, expressed concern that cyber operations are increasingly becoming part of conflicts and can disrupt vital services to civilians, including health and medical facilities that are particularly vulnerable to cyberattacks. Estonia highlighted malicious cyber activities targeting critical civilian infrastructure and stressed that existing international law applies in cyberspace, noting that strengthening the resilience of indispensable objects and essential services, including through cybersecurity, is integral to both conflict prevention and post-conflict recovery. India warned that civilians and critical civilian infrastructure in urban areas have become frequent targets in armed conflict, observing that cyberattacks against civilian infrastructure, including health-care systems, have become increasingly common and can compromise access to humanitarian assistance, including through attacks on hospitals, medical transport, and essential services.

[165] Security Council Meeting Record (8 November 2024) (S/PV.9779); see also UN Security Council Meeting Press Release. "Ransomware Attacks on Healthcare Sector 'Pose a Direct and Systemic Risk to Global Public Health and Security', Executive Tells Security Council" (8 November 2024) (SC/15891).

[166] Security Council Report. "Arria-formula Meeting on Cyber-Attacks Against Critical Infrastructure". What's in Blue. (25 August 2020).

[167] Security Council Report. "Arria-formula Meeting on "The Responsibility and Responsiveness of States to Cyberattacks on Critical Infrastructure"". What's in Blue. (25 May 2023).

[168] The agreed voluntary, non-binding norms provides that states should take appropriate measures to protect their critical infrastructure from ICT threats, should not conduct or knowingly support ICT activity contrary to their obligations under international law that intentionally damages critical infrastructure or otherwise impairs its use and operation in providing services to the public, and should respond to appropriate requests for assistance by another state whose critical infrastructure is subject to malicious ICT acts. See Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (22 July 2015) (A/70/174).

[169] UN Office for the Coordination of Humanitarian Affairs (OCHA) (May 2019). Building a Culture of Protection: 20 Years of Security Council Engagement on the Protection of Civilians.

[170] Richard Gowan (July 2019). "The Security Council and the Protection of Civilians" in Evolution of the Protection of Civilians in UN Peacekeeping, ed. Lisa Sharland (Stimson Center Special Report No. 140), pages 7–10.

[171] Final Report of the Open-ended Working Group on security of and in the use of information and communications technologies 2021–2025 (24 July 2025) (A/80/257).

[172] Report of the Secretary-General on the Protection of Civilians in Armed Conflict (15 May 2025) (S/2025/271).

[173] Ibid., para. 49.

assist populations in need.[174] Similar dynamics were reported in the Democratic Republic of the Congo (DRC), Ethiopia, the Occupied Palestinian Territory, and elsewhere.[175] In Ethiopia, humanitarian actors engaged with social media to secure the removal of threatening online content targeting aid workers. In response to this growing issue, the Secretary-General published a policy brief in June 2023 advancing a code of conduct for information integrity on digital platforms.[176] Through extensive multistakeholder dialogues, this evolved into a broader set of global principles for information integrity.[177]

These concerns have also become more visible in the Council's own deliberations, where misinformation, disinformation, and hate speech have increasingly been treated not only as enablers of terrorism, but also as broader drivers of conflict and threats to civilian protection and mission effectiveness. A notable development in this regard was the adoption of resolution 2686 (2023) on "tolerance and international peace and security". Co-authored by the UAE and the UK, the resolution expressed concern at instances of violence fuelled by hate speech, misinformation, and disinformation, including through social media platforms. It also recognised that hate speech, racism, racial discrimination, xenophobia, and related forms of intolerance, as well as "acts of extremism", could contribute to the outbreak, escalation, and recurrence of conflict, and it condemned misinformation, disinformation, and incitement to violence against UN peacekeeping operations intended to undermine their safety and ability to implement their mandates.[178] The resolution was adopted unanimously, though some members raised concerns in their explanations of vote about its scope and language.[179]

A June 2024 Council briefing on the implementation of resolution 2686 reinforced this framing, with speakers noting that the Council had since addressed misinformation, disinformation, and hate speech across multiple country-specific situations on its agenda, including the Central African Republic (CAR), the DRC, Libya, Somalia, South Sudan, and the Middle East.

The Council has also used informal formats to address the online dimension of these risks more directly. In October 2021, Kenya, together with the UN Office on Genocide Prevention and the Responsibility to Protect, organised a closed Arria-formula meeting on "Addressing and Countering Hate Speech and Preventing Incitement to Discrimination, Hostility, and Violence on Social Media". The meeting aimed to facilitate dialogue among Council members, the UN, and social media companies, including Facebook, Twitter, and TikTok, on improving responses to hate speech and incitement in conflict situations.[180]

The Council has also addressed the ways in which new technologies, particularly AI, could intensify these risks. Members have raised concerns about AI-enabled manipulation at scale, including the use of deepfakes and synthetic media to inflame tensions, discredit humanitarian actors, and shape public perceptions during conflict.[181] An Arria-formula meeting convened by Albania and the UAE in December 2023 on "Artificial intelligence: its impact on hate speech, disinformation and misinformation" illustrated the extent to which the integrity of public information is increasingly being viewed as part of the broader protection and conflict-prevention landscape.[182] In this regard, member states have noted that generative AI and large language models have lowered barriers to malicious ICT activities, while underscoring the importance of ensuring the safety and security of AI systems and the data used to train them.[183]

At the operational level, the Council has progressively integrated online information-related risks into the mandates of peacekeeping and special political mission. Resolution 2729 (2024) on the UN Mission in South Sudan (UNMISS), for example, called on all parties to refrain from destabilising activities, incitement to hatred and violence, and misinformation and disinformation campaigns aimed at the mission, including through social media.[184] In some more recent mandate negotiations, references to "misinformation and disinformation" were revised to formulations such as "false and falsified information".[185] This shift was evident, for example, in resolution 2779 (2025) on UNMISS, which called on parties to "refrain from spreading false and falsified information undermining UNMISS, including through social media",[186] and in resolution 2802 (2025) on the UN Interim Security Force in Abyei (UNISFA), which called for efforts to "promote information integrity and counter dissemination of false and falsified information".[187]

The Council has also sought to strengthen missions' capacity to monitor and respond to misinformation and disinformation, including through strategic communications. A presidential statement proposed by Brazil and adopted in July 2022 underscored the importance of strategic communications for effective mandate implementation and for responding to misinformation and disinformation affecting mission credibility, consent, and personnel safety.[188] This approach subsequently appeared across a range of mandates. Resolution 2723 (2024), for example, requested the UN Peacekeeping Force in Cyprus (UNFICYP) to strengthen its existing efforts to monitor and counter misinformation and disinformation. The Council similarly tasked MONUSCO, the UN

[174] Report of the Secretary-General on the Protection of Civilians in Armed Conflict (14 May 2024) (S/2024/385), para. 38.
[175] Report of the Secretary-General on the Protection of Civilians in Armed Conflict (15 May 2025) (S/2025/271), para. 38.
[176] Our Common Agenda | Policy Brief 8: Information Integrity on Digital Platforms (June 2023) (EOSG/2023/8).
[177] United Nations Global Principles for Information Integrity: Recommendations for Multi-Stakeholder Action (2024).
[178] Security Council Resolution 2686 (14 June 2023) (S/RES/2686).
[179] Some members raised concerns about the unqualified use of the term "extremism" and the risk of overly broad interpretation, including in ways that could affect freedom of expression. For example, France expressed regret that the draft resolution was "selective and too weak" on issues such as freedom of expression in all its forms and "a potentially too-broad conception of extremism". Switzerland also expressed concern that the term "extremism" without the qualification "violent" in the resolution, "leaves room for a broad interpretation that could be used arbitrarily against individuals and groups exercising their freedom of expression and opinion". Security Council Meeting Record (14 May 2023) (S/PV.9347).
[180] Security Council Report. "Arria-Formula Meeting on Hate Speech and Social Media". What's in Blue. (27 October 2021).
[181] While not explicitly linked to ICTs, Security Council resolution 2730 (2024) condemned disinformation, information manipulation, and incitement to violence against humanitarian and UN personnel.
[182] Security Council Report. "Arria-Formula Meeting on Artificial Intelligence: Its Impact on Hate Speech, Disinformation and Misinformation". What's in Blue. (18 December 2023).
[183] Final Report of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025 (24 July 2025) (A/80/257); Report of the Secretary-General on Artificial Intelligence in the Military Domain and its Implications for International Peace and Security (5 June 2025) (A/80/78).
[184] Security Council Resolution 2729 (29 April 2024) (S/RES/2729).
[185] Security Council Report. "UN Mission in South Sudan (UNMISS): Vote on Mandate Renewal Resolution". What's in Blue. (8 May 2025).
[186] Security Council Resolution 2779 (8 May 2025) (S/RES/2779).
[187] Security Council Resolution 2802 (14 November 2025) (S/RES/2802).
[188] Statement by the President of the Security Council (12 July 2022) (S/PRST/2022/5).

Interim Force in Lebanon (UNIFIL), Multidimensional Integrated Stabilization Mission in the Central African Republic (MINUSCA), UNISFA, and UN Integrated Office in Haiti (BINUH) with enhancing strategic communications and countering disinformation, particularly where such campaigns undermine civilian protection, political processes, mandate implementation, or the safety of UN personnel.[189] In some cases, such as MONUSCO and MINUSMA, these tasks were linked explicitly to disengagement or withdrawal phases, in which misinformation and disinformation could heighten risks to civilians and UN staff.[190]

Lethal Autonomous Weapons Systems

The Security Council's consideration of technology-related threats to the protection of civilians has increasingly extended to the military applications of AI and autonomous weapons systems (AWS), including those with lethal effects. Although there is no internationally agreed-upon definition of AWS or lethal autonomous weapons systems (LAWS), such systems are often described as weapons that, once activated, can select and engage targets without further human intervention.[191] States have long fielded weapons with limited autonomous functions, but more recent developments have involved increasingly sophisticated systems capable of operating with greater autonomy, in complex environments, and without Internet connectivity.[192] While AI is not a prerequisite for autonomy, its integration can enable systems to process information and operate at greater speed and scale, raising distinct humanitarian, legal, and ethical concerns.[193]

These concerns were evident in the range of views that states have expressed on the implications of LAWS for international peace and security. In his 2024 report on LAWS, the Secretary-General noted concerns that such systems could have destabilising effects, lower the threshold for the use of force, increase the frequency and intensity of conflict, and heighten escalation risks because of their unpredictability, including through machine-to-machine interaction and the increased speed of warfare.[194] States also warned of the risk of an arms race, the possibility that such systems could be fitted with nuclear weapons or other weapons of mass destruction, and the danger of their acquisition by non-state actors, including terrorist and criminal groups. Some further raised concerns about possible use in domestic law enforcement and the related human rights implications.

At the same time, some states saw possible military advantages in AWS, including gains in safety, efficiency, and precision, and potential improvements in compliance with IHL and the protection of civilians. The ICRC has cautioned, however, that claims that new weapons will be more humane, less lethal, and more precise have long accompanied the promotion of new military technologies, but that this is not what has been seen historically. It also urged states to conclude a treaty on AWS and adopt a human-centred approach to military AI.[195]

From a PoC perspective, the military use of AI and AWS has raised particular concerns about compliance with IHL and the degree of human oversight in decisions on the use of force. The Secretary-General's 2025 report on PoC noted that, while AI could help anticipate and avoid civilian harm, it had also reportedly been used in armed conflict to select targets and make life-or-death decisions at high speed and volume, increasing the risks to civilians. The report further underscored that this raised serious concerns regarding compliance with international law, including because of the difficulty of predicting AI outputs and the risks associated with automation bias.[196]

These concerns were not merely hypothetical. In its March 2021 final report, the Panel of Experts on Libya reported that, during the 2020 hostilities, retreating forces were "hunted down and remotely engaged" by unmanned combat aerial vehicles or "lethal autonomous weapons systems", and that such systems were "programmed to attack targets without requiring data connectivity between the operator and the munition", amounting "in effect" to a "fire, forget and find" capability.[197] Although the report did not establish the precise degree of human involvement in individual engagements, it underscored the operational relevance of increasing autonomy in weapons systems in active conflict settings and the implications for civilian protection. More recent media reporting has also pointed to the growing use of AI-enabled, and increasingly autonomous, military systems in ongoing conflicts, underscoring the continued relevance of these concerns.[198]

The Secretary-General has repeatedly stated that machines with the power and discretion to take human lives without human control are politically unacceptable and morally repugnant, and should be banned under international law.[199] In his New Agenda for Peace and subsequent reports, he called on states to conclude by 2026 a legally binding instrument prohibiting AWS that function without human control or oversight and cannot be used in compliance with IHL, while regulating all other types of AWS.[200]

[189] Security Council Resolution 2666 (20 December 2022) (S/RES/2666), para. 24(f); Security Council Resolution 2650 (31 August 2022) (S/RES/2650), para. 24; Security Council Resolution 2659 (14 November 2022) (S/RES/2659), para. 32; Security Council Resolution 2630 (12 May 2022) (S/RES/2630), para. 5; and Security Council Resolution 2743 (12 July 2024) (S/RES/2743), para. 1.

[190] In connection with MINUSMA, Security Council Resolution 2690 (30 June 2023) (S/RES/2690), para. 6(vi); and, in connection with MONUSCO, Security Council Resolution 2717 (19 December 2023) (S/RES/2717), paras. 27 and 34(i) (f). The Council placed special emphasis on the protection of civilians and United Nations and humanitarian personnel in the context of the withdrawal of MINUSMA from Mali and of MONUSCO from South Kivu in the Democratic Republic of the Congo.

[191] Report of the Secretary-General on Lethal Autonomous Weapons Systems (1 July 2024) (A/79/88).

[192] Advances in edge AI, which allow AI processing on devices without reliance on internet connectivity, have accelerated this trend. See Wenting He (2024). Enabling Technologies and International Security: A Compendium (2024 edition). Geneva, Switzerland: UNIDIR.

[193] UNODA. "Lethal Autonomous Weapon Systems".

[194] Report of the Secretary-General on Lethal Autonomous Weapons Systems (1 July 2024) (A/79/88).

[195] Security Council Meeting Record (25 September 2025) (S/PV.10005 (Resumption I)).

[196] Report of the Secretary-General on the Protection of Civilians in Armed Conflict (15 May 2025) (S/2025/271).

[197] Letter dated 8 March 2021 from the Panel of Experts on Libya established pursuant to resolution 1973 (2011) addressed to the President of the Security Council (8 March 2021) (S/2021/229), para. 63.

[198] See, for example, Volodymyr Pavlov (29 November 2025). "Ukrainian drone pilots look to AI for battlefield edge". Reuters; Michael Biesecker et al. (18 February 2025). "As Israel uses U.S.-made AI models in war, concerns arise about tech's role in who lives and who dies". Associated Press; and Sheera Frenkel and Natan Odenheimer (25 April 2025). "Israel's A.I. Experiments in Gaza War Raise Ethical Concerns". New York Times.

[199] Secretary-General Statement and Messages. "Lethal Autonomous Weapon System 'Politically Unacceptable, Morally Repugnant and Should Be Banned', Secretary-General Says during Informal Consultations on Issue" (12 May 2025) (SG/SM/22643).

[200] UNODA. "Lethal Autonomous Weapon Systems"; Our Common Agenda | Policy Brief 9: A New Agenda for Peace (June 2023) (EOSG/2023/9), page 27.

While the Security Council has not yet held a meeting specifically dedicated to LAWS, the issue has surfaced in thematic discussions on new and emerging technologies. In those settings, some members highlighted the risks associated with the misuse and potential weaponisation of emerging technologies, including AI, and underscored the need for human oversight in decision-making, arguing that responsibility and accountability should not be delegated to machines.[201] These interventions suggested growing awareness within the Council of the civilian protection implications of increasingly autonomous weapons systems.

Concerns regarding the military applications of AI have also been taken up by the General Assembly, which adopted resolutions in December 2024 and December 2025 on “Artificial intelligence in the military domain and its implications for international peace and security”. The resolutions requested the Secretary-General to seek the views of member states on the opportunities and challenges that the application of AI in the military domain poses for international peace and security, with a specific focus on areas other than LAWS, and to submit a substantive report on those views and on existing and emerging normative proposals for further discussion.

In relation to LAWS, the main multilateral forum remains the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, established by the High Contracting Parties to the CCW. Since its creation in 2017, the Group has served as the central platform for technical, legal, and policy discussions on LAWS.[202] The Secretary-General’s 2024 report on LAWS showed that some states were open to parallel discussions outside the CCW framework where such engagement could support the Group’s work, including by enhancing inclusivity and enabling linkages to related issues. Others cautioned against parallel processes that could prove counterproductive and fragment international efforts.[203] These differing views echoed broader debates about the respective roles of different UN organs and forums, including the Security Council, in addressing risks associated with new and emerging technologies.

Technology and Sanctions

Security Council sanctions regimes have been used to address an increasingly broad range of issues, from illicit arms flows and serious human rights abuses, to the illicit exploitation of natural resources, criminal networks and trafficking, and conflict-related sexual and gender-based violence.[204] In recent years, technology-related considerations have become more visible within the Council’s sanctions architecture. They have emerged mainly through the work of sanctions committees and panels of experts, particularly where new technologies enable designated actors to finance operations, evade restrictions, or enhance operational capabilities.

Early recognition of these considerations could be seen in the High-Level Review of UN Sanctions, whose findings were consolidated in the Compendium circulated in 2015.[205] Although the Review was not centred on technology as a distinct thematic issue, it examined emerging challenges associated with the use of the Internet and ICTs in sanctions implementation. It highlighted, in particular, the use of the Internet and ICTs for propaganda, the circulation of hate speech, and the recruitment and financing of violent extremism. The Compendium also pointed to the need for export control regimes to keep pace with technological developments, including 3D-printed weapons, modular weapons, and the online availability of technical know-how for weapons manufacturing. While the Review did not lead to an ongoing follow-up process on these issues within the UN sanctions architecture, it anticipated a number of technology-related challenges that later became more prominent in sanctions-related reporting and implementation discussions.[206]

The ISIL (Da’esh) and Al-Qaida sanctions regime provides a clear example of how the security implications of technological developments have entered Council sanctions practice.[207] Since at least 2015, the Council has confirmed that the assets-freeze obligation applies to financial and economic resources of every kind, including those used for the provision of “Internet hosting and related services” when used to support listed individuals and entities.[208]

Recent reports of the ISIL (Da’esh) and Al-Qaida Sanctions Committee’s Analytical Support and Sanctions Monitoring Team have documented terrorist groups’ exploitation of ICTs, including social media and online financial tools.[209] They have highlighted the use of online mechanisms for fundraising, including through virtual assets, and noted the growing use of “anonymity-enhancing” cryptocurrencies to obscure transaction trails and complicate the implementation of asset-freeze measures.[210]

Sanctions reporting has also highlighted how sanctioned actors exploit new technologies. The Analytical Support and Sanctions Monitoring Team has drawn attention to terrorist development of unmanned aerial and maritime weapons and surveillance systems, as well as the potential use of 3D printing to circumvent restrictions imposed under the ISIL (Da’esh) and Al-Qaida sanctions regime.[211] One member state reported to the Monitoring Team that Al-Shabaab was experimenting with 3D printing to manufacture components for adapting commercial UAS. Such reporting illustrates how computer code developed in a secure environment could be disseminated to

[201] Security Council Meeting Record (22 May 2025) (S/PV.9921): open debate on protection of civilians in armed conflict. See, for example, the statement made by China and Denmark.
[202] UNODA. “Convention on Certain Conventional Weapons – Group of Governmental Experts on Lethal Autonomous Weapons Systems (2025)”. UNODA Meetings Place.
[203] Report of the Secretary-General on Lethal Autonomous Weapons Systems (1 July 2024) (A/79/88).
[204] See, for example, S/RES/2174 (27 August 2014); S/RES/2213 (27 March 2015); S/RES/2293 (23 June 2016); S/RES/2521 (29 May 2020); S/RES/2653 (21 October 2022); S/RES/2794 (17 October 2025).
[205] High-Level Review of United Nations Sanctions (2015). Compendium of the High-Level Review of United Nations Sanctions, sponsored by the Governments of Australia, Finland, Germany, Greece and Sweden: launched at the United Nations on 28 May 2014; and Letter dated 12 June 2015 from the Permanent Representatives of Australia, Finland, Germany, Greece and Sweden to the UN addressed to the Secretary-General (A/69/941–S/2015/432).
[206] Camino Kavanagh (2017). The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century, Geneva, Switzerland: UNIDIR.
[207] The ISIL (Da’esh) and Al-Qaida sanctions regime is overseen by the Security Council Committee pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015).
[208] Security Council Resolution 2253 (17 December 2015) (S/RES/2253).
[209] Thirty-fifth Report of the Analytical Support and Sanctions Monitoring Team submitted pursuant to resolution 2734 (2024) concerning ISIL (Da’esh), Al-Qaida and associated individuals and entities (6 February 2025) (S/2025/71); and Thirty-fourth Report of the Analytical Support and Sanctions Monitoring Team submitted pursuant to resolution 2734 (2024) concerning ISIL (Da’esh), Al-Qaida and associated individuals and entities (19 July 2024) (S/2024/556).
[210] Ibid.; and Thirty-second Report of the Analytical Support and Sanctions Monitoring Team submitted pursuant to resolution 2610 (2021) concerning ISIL (Da’esh), Al-Qaida and associated individuals and entities (24 July 2023) (S/2023/549).
[211] Thirty-fourth Report of the Analytical Support and Sanctions Monitoring Team submitted pursuant to resolution 2734 (2024) concerning ISIL (Da’esh), Al-Qaida and associated individuals and entities (19 July 2024) (S/2024/556).

terrorists in the field and used to print components for attack devices, including improvised explosive devices and weaponised UAS, potentially circumventing arms restrictions.

Recent Monitoring Team reports have also noted that listed groups have experimented with AI, primarily for radicalisation, recruitment, and propaganda amplification. Al-Shabaab, for example, reportedly used AI tools to translate a series of messages into multiple languages, while ISIL (Da'esh) experimented with AI-generated fake documentation to bypass identity checks. ISIL (Da'esh) also reportedly circulated guidance on how to use generative AI, including ChatGPT, while avoiding detection, and sought to recruit cyber experts to strengthen these capabilities. Although these developments have not yet resulted in specific sanctions measures targeting AI-related activity, they have informed the analytical baseline for assessing evolving threats and implementation challenges.

The Council has nevertheless addressed concerns regarding terrorist use of ICTs in resolutions renewing the ISIL (Da'esh) and Al-Qaida sanctions regime. Resolution 2610 (2021), for example, expressed concern at terrorists' increased use of ICTs, in particular the Internet, including to facilitate recruitment, fundraising, and the planning of terrorist acts, and underscored the importance of cooperative action to counter such use.[212] Resolution 2734 (2024) broadened this language to include "other new and emerging technologies", while reaffirming that measures to counter terrorist use of such technologies should remain consistent with obligations under international law, including international human rights law.[213]

Country-specific sanctions regimes have further illustrated the operational implications of new technologies. In Haiti, reports of the Panel of Experts established pursuant to resolution 2653 (2022) have documented gangs' procurement of commercial drones for surveillance and the coordination of attacks, which significantly enhanced their operational capacity. Although commercial drones are not specifically covered by the arms embargo, the Panel noted that their provision to gangs constitutes assistance to criminal groups and could therefore meet designation criteria.[214] Similarly, reports of the Panel of Experts on Yemen, submitted to the Committee established pursuant to resolution 2140 (2014), has documented the development and use of missile and drone capabilities.[215]

Case Study: The 1718 Committee and Cyber-enabled Sanctions Evasion

The Democratic People's Republic of Korea (DPRK) sanctions regime stands out as one of the clearest examples of the Council's engagement with cyber activities explicitly framed as sanctions evasion. For years, reports of the Panel of Experts assisting the Committee established pursuant to resolution 1718 (2006) documented the DPRK's use of cyber operations to generate revenue, gain access to financial systems, and circumvent sanctions. They described a range of activities, including cyber-enabled theft from financial institutions and virtual asset service providers, spear-phishing and other social-engineering campaigns, ransomware incidents, and cyber-espionage targeting governments and other entities involved in sanctions implementation.[216]

Successive Panel reports also documented the scale and growing sophistication of DPRK cyber operations, including estimates of illicit revenue from cyber-enabled theft ranging from hundreds of millions to over a billion dollars in particular reporting periods.[217] The Panel assessed that such activity offered a low-risk, high-reward means of generating revenue and evading sanctions, and that the proceeds contributed to financing the DPRK's prohibited weapons programmes. Its reporting also included recommendations to strengthen implementation, including enhanced information-sharing, improved cyber hygiene, and engagement with the private sector, including virtual asset service providers, to help mitigate cyber-enabled sanctions evasion.[218]

Despite the prominence of cyber issues in Panel reporting and Committee discussions, these concerns did not translate into Council outcomes. A draft resolution tabled by the US in May 2022 would have strengthened the DPRK sanctions regime by, among other measures, designating the Lazarus Group, described in the draft as subordinate to the Reconnaissance General Bureau, the DPRK's primary intelligence agency, and by introducing operative language on "malicious cyber activity".[219] The draft called on member states to take "appropriate measures", within their jurisdiction and in accordance with their respective legal processes, to prevent the DPRK and its nationals from using their territories to conduct or facilitate malicious ICT activity for the purposes of sanctions evasion and contributing to the DPRK's nuclear and ballistic missile programmes. It clarified that such measures "could include but are not limited to" repatriating DPRK nationals engaged in such activity and closing businesses associated with them. It also called on the DPRK to adhere fully to the UN General Assembly-affirmed framework of responsible state behaviour in cyberspace and its voluntary norms and underscored the applicability of international law in cyberspace.

It appears that language concerning the DPRK's malicious cyber activity enjoyed strong support among Council members during the negotiations. Following concerns about the practical implications of this approach, the draft was amended to clarify that the examples of measures states could take were illustrative rather than prescriptive.[220]

Ultimately, the draft resolution was not adopted, as China and Russia cast a veto while the other 13 Council members voted in favour.[221] Had it been adopted, however, the resolution would have marked a notable instance of the Council operationalising, in a sanctions context, an agreed voluntary norm of responsible state behaviour in cyberspace, namely that states should not knowingly allow their territory to be used for internationally wrongful acts using ICTs.[222]

Hate Speech, Digital Platforms and Designation Criteria

As noted in the section on the protection of civilians, technology can amplify the reach and impact of incitement and hate-based messaging, including through both broadcast and online channels. Within sanctions practice, an early example was resolution 1572 (2004) on Côte d'Ivoire, which demanded an end to radio and

[212] Security Council Resolution 2610 (17 December 2021) (S/RES/2610).

[213] Security Council Resolution 2734 (10 June 2024) (S/RES/2734).

[214] Letter dated 25 September 2025 from the Panel of Experts established pursuant to Security Council resolution 2653 (2022) addressed to the President of the Security Council (S/2025/597).

[215] Security Council Committee established pursuant to Security Council Resolution 2140 (2014).

[216] Letter dated 7 March 2024 from the Panel of Experts established pursuant to resolution 1874 (2009) addressed to the President of the Security Council (S/2024/215); and Letter dated 28 August 2020 from the Panel of Experts established pursuant to resolution 1874 (2009) addressed to the President of the Security Council (S/2020/840).

[217] Report of the Panel of Experts established pursuant to resolution 1874 (2009) (7 March 2023) (S/2023/171); and Report of the Panel of Experts established pursuant to resolution 1874 (2009) (7 March 2024) (S/2024/215).

[218] Ibid.

[219] Draft Security Council Resolution (26 May 2022) (S/2022/431). See section entitled "Malicious Cyber Activity".

[220] Security Council Report. "DPRK/North Korea: Yesterday's Vote on a Sanctions Resolution". What's in Blue. (31 May 2022).

[221] Security Council Meeting Record (26 May 2022) (S/PV.9048).

[222] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (22 July 2015) (A/70/174).

television broadcasts inciting hatred and violence and included among the designation criteria individuals who "incite publicly hatred and violence".[223] In the case of South Sudan, resolution 2206 (2015) condemned the use of the media to spread hate speech and incite violence, while subsequent reporting by the Panel of Experts assisting the Committee established pursuant to that resolution documented cyber incidents and online harassment affecting journalists and online activists.[224]

Technology and Peacekeeping

In recent decades, the gradual integration of technology into UN peacekeeping has been shaped by operational needs and Secretariat-led reform initiatives, with periodic engagement by the Security Council. This integration was driven by a growing recognition that peace operations increasingly depend on timely and reliable information, effective communications, and stronger analytical capabilities to operate in complex and volatile environments.

By the early 2010s, as peacekeeping mandates became more multidimensional and missions were deployed in increasingly insecure settings marked by asymmetric threats, shortcomings in information management and situational awareness had become more apparent. In December 2012, against the backdrop of the deteriorating security situation linked to the M23 crisis in the DRC, the Secretary-General set out options to improve the ability of MONUSCO to implement its mandate, including through additional "force multipliers". Among the measures proposed was the strengthening of the mission's information capabilities, including the use of unmanned aerial systems (UAS) for surveillance to support information collection, analysis, and dissemination, enhance situational awareness, and enable more timely decision-making.[225]

The Council responded in January 2013, in an exchange of letters with the Secretary-General, by taking note of the Secretariat's intention to use such assets in the DRC on a case-by-case basis, while stressing that this was without prejudice to the ongoing consideration by relevant UN bodies of the legal, financial, and technical implications of UAS use.[226] Resolution 2098 (2013) subsequently incorporated these surveillance capabilities into MONUSCO's mandate, deciding that the mission should monitor implementation of the arms embargo, in particular the flows of military personnel, arms, or related materiel across the eastern border of the DRC, including through UAS-based surveillance.[227]

In 2013 and 2014, technology featured more prominently in the work of the Council and its subsidiary bodies. In July 2013, the Working Group on Peacekeeping Operations, chaired by Pakistan, held a dedicated meeting on the use of modern technology in UN peacekeeping, at which the Under-Secretary-General for Peacekeeping Operations and the Under-Secretary-General for Field Support described how technology was supporting a wide range of military, police, and civilian tasks. They referred to tools such as geographic information systems, encrypted communications, ground surveillance radar, helmet cameras, night-vision equipment, electronic trackers, advanced vehicle armour, and unarmed UAS.[228] In other Council discussions, including a June 2013 briefing on UN peace operations, Force Commanders and Secretariat officials highlighted the operational value of improved information and situational awareness for early warning, the safety and security of personnel, and more effective mandate implementation.[229]

In parallel, the Secretariat, through the Departments of Peacekeeping Operations and Field Support, sought to strengthen the technological foundations of peacekeeping, including by commissioning an independent Expert Panel on Technology and Innovation in UN Peacekeeping in June 2014.[230] In its final report, issued in December 2014, the Panel concluded that UN peacekeeping remained "well behind the curve" in adopting modern technologies and called for a more sustained and systematic approach to innovation. Its proposals included identifying "technology-contributing countries" (TechCCs), advancing the concept of the "Digital Peacekeeper", equipped with up-to-date technologies and supported by training and periodic review, and establishing guiding assumptions and principles for the deployment and use of modern technology, including a high degree of transparency.

From the mid-2010s onward, engagement by the Secretariat and the Security Council shifted from consideration of specific tools toward more integrated approaches to digital transformation. System-wide initiatives of the Secretary-General—including the Strategy on New Technologies (2018), the report of the High-level Panel on Digital Cooperation (2019), the Roadmap for Digital Cooperation (2020), and the Data Strategy for Action (2020)—marked a growing focus on harnessing digital and emerging technologies in support of UN mandates and the 2030 Agenda for Sustainable Development. In the context of peacekeeping, this broader shift was also evident in resolution 2518 (2020), in which the Council took note of the Secretary-General's ongoing work to develop a strategy for integrating new technologies to improve safety and security, situational awareness, field support, and substantive mandate implementation.[231]

This shift found more concrete expression in the 2021 Strategy for the Digital Transformation of UN Peacekeeping. The Strategy framed digital transformation as a broader process of change within the UN, driven and enabled by digital technologies and involving a significant measure of cultural change. It envisaged digital technologies as an enabler for UN peacekeeping, supporting analysis-driven and forward-looking understanding of conflict environments, strengthening the safety and security of personnel, and shaping agile and responsive mandate implementation.[232] It also set out principles for the responsible use of technology and data in peacekeeping, including data protection and privacy, do-no-harm, and human-centred approaches, and identified the need to address evolving risks in the digital environment, including misinformation, disinformation, and cyberattacks.

[223] Security Council Resolution (15 November 2004) (S/RES/1572).
[224] Letter dated 26 April 2023 from the Panel of Experts on South Sudan addressed to the President of the Security Council (S/2023/294).
[225] Letter dated 27 December 2012 from the Secretary-General addressed to the President of the Security Council (S/2013/43).
[226] Letter dated 22 January 2013 from the President of the Security Council addressed to the Secretary-General (S/2013/44).
[227] Security Council Resolution (28 March 2013) (S/RES/2098)
[228] Letter dated 31 December 2013 from the Chair of the Security Council Working Group on Peacekeeping Operations addressed to the President of the Security Council (S/2013/786).
[229] Security Council Report. "Peacekeeping Working Group Meeting on the Use of Technology". What's in Blue (18 July 2013).
[230] Final Report of the Expert Panel on Technology and Innovation in UN Peacekeeping (22 December 2014).
[231] Security Council Resolution (30 March 2020) (S/RES/2518).
[232] Strategy for the Digital Transformation of UN Peacekeeping (August 2021).

Security Council engagement during the same period reinforced this framing. In August 2021, under India's presidency, the Council held a ministerial-level open debate on "Protecting the protectors: technology and peacekeeping" and adopted a presidential statement recognising technology's potential to act as a "force multiplier". The text noted that technology could help missions develop a deeper understanding of their operating environments through improved data collection, analysis, and dissemination, and by enabling more effective and timely decision-making through early warning and response.[233] During the debate, some members stressed that the integration of modern technologies into peacekeeping should remain consistent with peacekeeping principles, including respect for host-state sovereignty and consultation with host countries.[234]

Technology as an Enabler and a Threat in UN Peacekeeping

Security Council discussions, together with related Secretariat guidance and practice, have highlighted a range of ways in which technology can act as a force multiplier in peacekeeping. These include surveillance and monitoring tools, as well as platforms that help missions collect, integrate, and analyse data in support of early warning, situational awareness, and performance assessment.

In particular, intelligence, surveillance, and reconnaissance (ISR) capabilities expanded both the range and timeliness of information available to peacekeeping operations. Missions increasingly drew on geospatial tools, satellite imagery, digital mapping, unarmed UAS, and other sensors[235] to observe remote or inaccessible areas, monitor movements, and support mission and patrol planning.[236] These capabilities have been especially valuable for early warning and the protection of civilians when the information they generate is timely, reliable, and integrated into decision-making.[237] UN field missions and the Council's sanctions committees have also routinely used imagery intelligence in support of fact-finding and evidence-based reporting.[238]

Among these tools, UAS have remained one of the most visible manifestations of technological integration in peacekeeping. They can observe incidents in real time and monitor areas that are too remote, difficult, or dangerous for ground patrols to reach.[239] They have also been used to monitor the positions of opposing forces and illegal armed groups, track intrusions across demilitarised borders and buffer zones, detect and deter illegal activity, and help protect peacekeepers.[240] Their operational value has therefore made them an increasingly important part of the peacekeeping toolkit.

At the same time, the operational environment has evolved in ways that make technology not only a force multiplier, but also a threat to mandate implementation and the safety of UN personnel. In February 2024, UN peacekeepers in MONUSCO came under direct attack from UAS modified to deliver explosives. Several other missions have also documented an increase in UAS sightings within their areas of operation.[241] In its proposed programme budget for 2026, the Secretariat stressed that the growing threat posed by such systems required the development of counter-UAS capabilities in peace operations to ensure adequate protection for UN personnel.[242] The Council has also taken note of these developments, including by explicitly condemning drone attacks on UN personnel.[243]

This dual role of technology as both enabler and potential risk is particularly evident in the information environment.[244] Disinformation campaigns conducted through the Internet and social media can erode public trust in UN peace operations, affecting both mandate implementation and the safety and security of UN personnel.[245] Surveys conducted in 2024 indicated that nearly all peacekeeping missions perceived a growing prevalence of misinformation and disinformation in their operational environments, with 44 percent of personnel in the four largest missions reporting observable growth in such harmful content.[246]

False or misleading narratives have at times contributed to violence, resulting in fatalities among peacekeepers and civilians, damage to UN assets, and psychological strain that undermined mission morale. In the DRC, increased negative sentiment toward MONUSCO in July 2022 coincided with violent protests that led to the deaths of civilians and peacekeepers and severely disrupted mission operations, with around 400 UN vehicles immobilised because of security risks. In Lebanon, a disinformation campaign in December 2022 preceded a violent attack in Aqibiyah, southern Lebanon, in which one UNIFIL peacekeeper was killed and three others were injured. During the 2023 drawdown of MINUSMA in Mali, a surge in false and misleading narratives fuelled hostility toward peacekeepers and heightened concerns about the safety and security of mission personnel.[247]

In response, the Council has progressively integrated online information-related risks into the mandates of peacekeeping and political missions and sought to strengthen missions' ability to monitor and respond to misinformation and disinformation through enhanced strategic communications.

[233] Statement by the President of the Security Council (18 August 2021) (S/PRST/2021/17).

[234] Security Council Meeting Record (18 August 2021) (S/PV.8838): See statements by China, Kenya, and Russia.

[235] See UN Department of Peace Operations (DPO) (May 2025). Peacekeeping-Intelligence, Surveillance and Reconnaissance Staff Handbook (PKISR HB), 2nd ed., noting that, in addition to electro-optical sensors, peacekeeping ISR assets may use infra-red sensors, which detect emitted heat energy, and radar sensors, including synthetic aperture radar, typically carried on manned PKISR aircraft or larger UAS.

[236] Ibid.; and UN Department of Peace Operations (DPO) (2025). United Nations Military Peacekeeping Intelligence Handbook, 2nd ed.

[237] Agathe Sarfati (September 2023). New Technologies and the Protection of Civilians in UN Peace Operations, New York: International Peace Institute (IPI).

[238] Geospatial Information Section (GIS), Technology Operations Service (TOS), Operations Support Division (OSD) of the UN Office of Information and Communication Technology (OICT) (March 2021). Geospatial Strategy for the United Nations.

[239] UN Department of Peace Operations (DPO) (May 2025). Peacekeeping-Intelligence, Surveillance and Reconnaissance Staff Handbook (PKISR HB), 2nd ed.

[240] UN Department of Peace Operations (DPO) (December 2024). Current and Emerging Uniformed Capability Requirements for United Nations Peacekeeping; UN Department of Peace Operations (DPO) (May 2025). Peacekeeping-Intelligence, Surveillance and Reconnaissance Staff Handbook (PKISR HB), 2nd ed.

[241] Including: UNISFA, MINUSCA, UNIFIL, UNFICYP, and the UN Disengagement Observer Force (UNDOF).

[242] Proposed Programme Budget for 2026 | Part 2: Political affairs, Section 5: Peacekeeping operations, and Programme 4: Peacekeeping operations (30 April 2025) (A/80/6 (Sect. 5)).

[243] Security Council Press Statement on Drone Attacks on UNISFA Peacekeepers (19 December 2025) (SC/16259). The Council "unequivocally condemned in the strongest terms the heinous and deliberate 13 December drone attacks against the United Nations logistics base in Kadugli, South Kordofan, Sudan, which killed six Bangladeshi peacekeepers and injured nine others".

[244] Claire Wardle and Hossein Derakhshan (2017). Information Disorder: Toward an Interdisciplinary Framework for Research and Policymaking, Strasbourg: Council of Europe (2nd rev. ed., 2018).

[245] United Nations Peacekeeping. "Information Integrity and Harmful Information".

[246] Ibid.

[247] Ibid.

Missions have also increasingly built the capacity to monitor and analyse the information environment.[248] UN peacekeeping operations use a range of digital tools to track social media and other online content, including the Monitoring and Analysis of the Information Environment (MAIE) platform developed by the UN Department of Peace Operations (DPO) and UN Office for Information Communications Technology (OICT), which applies advanced analytics to monitor online discourse and identify harmful narratives and patterns of inauthentic behaviour across digital spaces.[249] These tools could support more preventive action, including targeted communications, closer engagement with vulnerable communities, and operational adjustments in at-risk areas.

Beyond information gathering, the Secretariat has also invested in platforms designed to organise and analyse operational data more systematically. The Situational Awareness Geospatial Enterprise (SAGE), first rolled out in 2015, provides a database for logging incidents, events, and activities, helping missions visualise hotspots, track trends, and strengthen situational awareness and early warning.[250] Another platform, Unite Aware, brought together different types of information, including SAGE incident reports, patrol planning data, geospatial information, imagery, geo-enabled sensor data, and video feeds, into a single web-based mapping system. Tested first in MINUSCA in 2019, it was gradually introduced in other missions.[251] The value of these systems, however, depends heavily on the timeliness, reliability, and consistency of data entry, as well as on common standards, interoperability, and mission leaders' ability to interpret and use the data effectively in decision-making.[252]

A related development was the Comprehensive Planning and Performance Assessment System (CPAS), first employed by the UN in 2018, which has helped missions connect information about the country situation with planning, data, results, and reporting. Its purpose was to support evidence-based assessments of mission impact and performance and to inform future planning.[253] Missions have increasingly relied on CPAS data and impact assessments to inform member states, including through the use of data, analysis, and visualisations in the Secretary-General's reports and fact sheets prepared for Security Council briefings. As at October 2025, six missions regularly included data visualisations in their reports, and 28 fact sheets had been prepared to support Security Council and other high-level briefings.[254]

The DPPA Innovation Cell's use of virtual reality (VR) tools shows how new technologies can also help bring field realities more directly into Council deliberations. Using VR headsets, Council members heard, in 2022, the perspective of various civil society actors involved in the peace process in Colombia and saw the damage from the war in Yemen. More recently, in February 2025, Council members used VR headsets to view the work of UNMISS in South Sudan, including conditions in flood-affected Bentiu, patrols along the Nile, and peacebuilding efforts in conflict-affected communities.[255] While not a substitute for in-person visits, such tools can offer a relatively cost-effective way for the Council to step up engagement with the field.[256]

While there is broad support within the Council for the view that technology can improve UN peacekeeping, some members have underscored the importance of ensuring that its use remains consistent with peacekeeping principles.[257] China and Russia, for example, have tended to emphasise host-state consent, sovereignty, and non-interference. At the Council's 18 August 2021 open debate on technology and peacekeeping, China argued that missions should consult host countries before using technologies for reconnaissance and surveillance and should refrain from harming the "national, public and information security" of host states.[258] Russia similarly argued that, while peacekeepers should be provided modern equipment, "the effectiveness of peacekeeping efforts does not always depend on technological equipment" and that "overcoming political tensions is the alpha and omega of UN effectiveness and its peacekeeping operations".[259]

These dynamics also surfaced during the negotiations on the Council's presidential statement on the impacts of scientific developments on peace and security, adopted on 21 October 2024.[260] It appears that early drafts included language expressing the Council's intention to anticipate and take into account more systematically the impact of scientific developments on the maintenance of international peace and security, including in efforts to enhance the effectiveness of peace operations, early warning, and conflict prevention and resolution. At the request of a Council member, however, the reference to peace operations, early warning, and conflict prevention

[248] UN Department of Peace Operations (DPO) (May 2025). Peacekeeping-Intelligence, Surveillance and Reconnaissance Staff Handbook (PKISR HB), 2nd ed, recommended that all missions consider employing a dedicated open-source peacekeeping intelligence analyst.

[249] Agathe Sarfati (September 2023). New Technologies and the Protection of Civilians in UN Peace Operations, New York: International Peace Institute, noting that UN peacekeeping operations have used a range of externally procured and platform-specific tools to monitor social media, including Logically AI, Crimson Hexagon, Dataminr, Predata, TalkWalker, Phoenix, Sparrow, and CrowdTangle. The paper also notes that DPO's focus has been on guiding missions in the use of such technologies rather than advocating the exclusive use of any one tool; Nana Appiah Acquaye (January 2026). "UN ICT tools Unite Wave and MAIE receive 2025 Secretary-General Award for combating Mis- and Disinformation". Review Tech Africa; and United Nations Peacekeeping. "Information Integrity and Harmful Information".

[250] UN Department of Operational Support (DOS), and UN Department of Management, Strategy, Policy and Compliance (2021). Strategy for the Digital Transformation of UN Peacekeeping, New York: United Nations, annex I.

[251] In Cyprus, for example, UNFICYP made daily use of Unite Aware to enhance situational awareness and analysis and finalised an innovative custom module on buffer zone management. MINUSCA leveraged newly available patrol planning and tracking features in Unite Aware to enhance operational planning and analysis. See: Report of the Secretary-General on the Implementation of the recommendations of the Special Committee on Peacekeeping Operations and its requests (13 October 2025) (A/80/439).

[252] Dirk Druet (April 2021). Enhancing the Use of Digital Technology for Integrated Situational Awareness and Peacekeeping-Intelligence, New York: United Nations; Allard Duursma and John Karlsrud (2019). "Predictive Peacekeeping: Strengthening Predictive Analysis in UN Peace Operations" in Stability: International Journal of Security & Development. 8, no. 1; Agathe Sarfati (September 2023). New Technologies and the Protection of Civilians in UN Peace Operations, New York: International Peace Institute (IPI).

[253] United Nations Peacekeeping. "CPAS"; United Nations Peacekeeping (2022). The Comprehensive Planning and Performance Assessment System (CPAS): Taking Stock Four Years after the Launch; UN Department of Peace Operations (DPO), UN Department of Operational Support (DOS), and UN Department of Management Strategy, Policy and Compliance (DMSPC) (2021). Strategy for the Digital Transformation of UN Peacekeeping, New York: United Nations, annex I.

[254] United Nations Peacekeeping (2022). The Comprehensive Planning and Performance Assessment System (CPAS): Taking Stock Four Years after the Launch; and Report of the Secretary-General on the Implementation of the recommendations of the Special Committee on Peacekeeping Operations and its requests (13 October 2025) (A/80/439).

[255] United Nations. "Virtual reality provides first-hand experience of UN peacekeeping". (11 February 2025).

[256] Security Council Report. "In Hindsight: The UN Security Council Returns to the Field". March 2023 Monthly Forecast. (28 February 2023).

[257] Statement by the President of the Security Council (18 August 2021) (S/PRST/2021/17).

[258] Security Council Meeting Record (18 August 2021) (S/PV.8838).

[259] Ibid.; Security Council Meeting Record (21 October 2024) (S/PV.9753): Russia further maintained that the Security Council should not encroach on the mandate of the General Assembly's Special Committee on Peacekeeping Operations (C34).

[260] Statement by the President of the Security Council (21 October 2024) (S/PRST/2024/6).

and resolution was removed. During the meeting held in connection with the adoption of the presidential statement, Russia argued that the Council should not encroach on the mandate of the General Assembly's Special Committee on Peacekeeping Operations (C34).

These dynamics also surfaced during the negotiations on the Council's presidential statement on the impacts of scientific developments on peace and security, adopted on 21 October 2024.[261] Early drafts apparently included language expressing the Council's commitment to take into account more systematically the impact of scientific developments on the maintenance of international peace and security. They also referred to doing so in efforts to enhance the effectiveness of peace operations, early warning, and conflict prevention and resolution. At the request of a Council member, however, that latter reference was removed. At the meeting held in connection with the adoption of the presidential statement, Russia argued that the Council "should not encroach" on the mandate of the General Assembly's Special Committee on Peacekeeping Operations (C34). It also maintained that it is not the Council's role to "discuss a new generation of soldiers and more effective fighters", suggesting that doing so is "antithetical to [the Council's] primary task of achieving a political solution to conflicts and peace".

Generative AI and Predictive Peacekeeping

The emergence of large language models (LLMs) such as ChatGPT has drawn greater attention to AI's potential to support human decision-making by processing and synthesising information far quicker and at greater scale than before. In peace operations, which generate large volumes of data and communications across multiple languages, generative AI could help automate routine information processing, support analysis, and improve efficiency in mandate implementation. This potential has become especially salient in a period of financial pressure and system-wide efforts to improve effectiveness, including through the Secretary-General's UN80 initiative. At the same time, the UN has stressed that AI can be both beneficial and harmful. At the Security Council's 18 July 2023 briefing on AI, for example, the Secretary-General said that, while AI could help identify patterns of violence, monitor ceasefires, and strengthen UN peacekeeping, mediation, and humanitarian efforts, it could also "amplify bias, reinforce discrimination, and enable new levels of authoritarian surveillance".[262]

For the Security Council, the significance of this development lies in the possibility that AI-enabled tools may improve the speed and quality of mission analysis, early warning, and reporting in support of mandate implementation and the Council's oversight of peace operations. Recent efforts across the Department of Political and Peacebuilding Affairs (DPPA) and DPO have focused on building staff skills and testing AI in limited ways as part of the broader digital transformation of peace operations. These include a structured pilot of Microsoft 365 Copilot with DPPA-DPO staff to assess productivity gains, operational implications, and information-security risks, as well as experimenting with narrowly scoped AI agents to support information retrieval and routine planning or reporting. In the field, missions also began developing more tailored tools. UNFICYP, for example, is building a knowledge hub agent designed to retrieve information and insights from its historical data, while MINUSCA is developing an AI agent to support more integrated analysis.

Discussions on future applications, while exploratory, have often focused on the possible integration of AI into existing platforms such as CPAS, Unite Aware, MAIE, and Unite Wave,[263] and on its potential to strengthen predictive analysis by synthesising multiple data sources in support of early warning, the safety and security of peacekeepers, and the protection of civilians.[264] Overall, the UN's approach has remained cautious and incremental, reflecting concerns about bias, opacity, data privacy, and the need to ensure human oversight of critical decisions, consistent with UN principles on the ethical use of AI.[265] More meaningful integration would also likely require stronger digital literacy, institutional adaptation, and sustained backing from member states, including through forums such as the C34, which considers developments in peacekeeping.[266]

Cybersecurity as a Potential Mandated Function of UN Peacekeeping

Forward-looking discussions on the future of peacekeeping have also examined whether UN missions might play a role in addressing emerging threats, including in the cyber domain. In this context, cybersecurity as a possible mandated function was suggested by the independent study commissioned by DPO to inform the May 2025 UN Peacekeeping Ministerial in Berlin, Germany.[267]

Launched on 1 November 2024, the study presented a range of models exploring how peace operations might adapt to evolving risk environments, including through roles related to infrastructure security and cybersecurity.[268] It envisaged a possible role in protecting elements of critical infrastructure necessary for the core functions of the state, including by helping secure locations and facilities such as airports, nuclear reactors, dams, medical facilities, urban settlements and cities, as well as undersea internet cables, electricity grids, and communication centres. It also outlined scenarios in which peacekeeping operations could, where mandated, contribute to upholding international law and implementing the agreed framework of responsible state behaviour in the use of ICTs. In some cases, according to the study, this could involve cyber means and methods used as part of a physical peace operation, or activities conducted in cyberspace with specialised expertise described as "digital blue helmets". More broadly, the study identified a spectrum of possible information security and cybersecurity-related tasks, ranging from preventing cyber intrusions and protecting information and computer systems and networks to conducting cyber operations for human protection purposes.[269]

[261] Statement by the President of the Security Council (21 October 2024) (S/PRST/2024/6).

[262] United Nations (18 July 2023). "Secretary-General's Remarks to the Security Council on Artificial Intelligence"; Security Council Meeting Record (18 July 2023) (S/PV.9381).

[263] Unite Wave is a technology tool that analyses FM radio broadcasts in dozens of local languages to combat misinformation and hate speech in peacekeeping settings.

[264] Generative AI may broaden the range of analytic tools that serve to forecast where and when armed violence will take place.

[265] Chief Executives Board for Coordination Summary of Deliberations: Principles for the Ethical Use of Artificial Intelligence in the United Nations System (27 October 2022) (CEB/2022/2/Add.1).

[266] Security Council Meeting Record (21 October 2024) (S/PV.9753).

[267] United Nations Peacekeeping. "United Nations Peacekeeping Ministerial 2025".

[268] UN Department of Peace Operations (DPO) (October 2024).The Future of Peacekeeping, New Models, and Related Capabilities, New York: United Nations.

[269] Additional functions described included preventing cyber intrusions; protecting information and computer systems and networks that are vital for sustaining life and livelihoods; providing technical assistance and advice to Member States; acting as trusted investigators by monitoring, analysing, and reporting on malicious activities and misinformation, disinformation,

The study garnered mixed reaction from member states. Some reportedly expressed scepticism about the feasibility of several of the proposed models, including those related to cybersecurity, while others viewed the study as a useful basis for discussions on possible future missions and how such models might work in practice.[270] Given current financial constraints and growing calls within the Council to refocus peace operations on core security and political tasks, it may be difficult for some of these models to gain traction in practice, at least in the near term.[271]

Technology and Women, Peace and Security

As digital technologies have become more central to social and political life, Council members and the Secretary-General have increasingly drawn attention to their implications for women's rights, safety, and participation in conflict and post-conflict settings. These include technology-facilitated gender-based violence, online harassment and intimidation, including against women in public and political spheres, and disinformation and hate speech that can reinforce discriminatory norms and deter women's civic engagement.[272] Several Council meetings have also highlighted the link between online and offline threats, including where digital harassment, doxing, and the non-consensual dissemination of intimate content can heighten risks to women's safety and contribute to wider constraints on civic space.[273]

At the same time, Council discussions and the Secretary-General's reporting have noted that digital tools can create opportunities relevant to the women, peace and security (WPS) agenda, including by expanding access to information and facilitating broader participation in political processes. Data-driven approaches have also been referenced in relation to early warning and the identification of patterns of sexual and gender-based violence, albeit alongside concerns about bias, exclusion, and unequal access.[274] The Secretary-General has underscored the importance of improving data availability and use as a structural enabler of the WPS agenda, including through his call for a "gender data revolution" on WPS to address persistent data gaps and strengthen accountability and decision-making.[275]

These issues have surfaced across the Council's WPS work through thematic debates, country-specific deliberations, and the Informal Expert Group (IEG) on WPS. In broader discussions on scientific and technological developments, some Council members have linked new and emerging technologies to questions of inclusion and gender equality and called for gender-sensitive approaches to ensure that technological advances benefit women and girls. At the Council's 21 October 2024 meeting on "Anticipating the impact of scientific developments on international peace and security", for example, Malta stressed the importance of ensuring women's full and equal participation in all processes related to emerging technologies, while Slovenia highlighted the potential use of advanced data analytics to identify patterns of sexual and gender-based violence and improve peacekeeping responses to threats facing people in vulnerable situations.[276]

Council discussions on digital technologies have also underscored their potential contribution to more inclusive political processes, including through large-scale online consultations designed to widen participation. At the Council's 23 May 2022 briefing on "Technology and security", Under-Secretary-General for Political and Peacebuilding Affairs Rosemary DiCarlo described the use of AI-assisted "digital dialogues" and online consultations in peace processes as a way to reach constituencies that are often excluded, including women.[277] She cited, for example, digital dialogues convened by the UN Support Mission in Libya (UNSMIL), each involving more than 1,000 participants, and online consultations through which the UN Special Envoy for Yemen engaged hundreds of women across different governorates to better understand the gendered dimensions of the conflict and the mediation process.[278]

Country-specific reporting and IEG discussions have provided more detailed examples of how ICT activity affected women's political participation and civic space. At a November 2023 IEG meeting on the DRC, participants reported that women electoral candidates faced hate speech and harassment both online and offline. They also noted that MONUSCO had shared information with the authorities on specific incidents and supported the establishment of women's situation rooms to help detect and respond to potential attacks against women voters, candidates, and electoral observers.[279]

Similar concerns surfaced in other IEG discussions. Council members have raised questions about the targeting of women human rights defenders and women in politics through disinformation and online harassment, including in Yemen.[280] The summary of the IEG's 30 September 2024 meeting on Myanmar also noted the online targeting of women associated with resistance movements, including the dissemination of sexually explicit images and threats of physical

malinformation, and hate speech (MDMH); helping secure computer systems and networks; offering targeted operational support to national authorities, including identifying and attributing specific threats; and perhaps even playing an active role in disrupting malicious cyber actors.

[270] Security Council Report. "In Hindsight: Ensuring Effective Peace Operations in an Uncertain World". Monthly Forecast (April 2025).

[271] Security Council Report. "In Hindsight: UN Peace Operations at a Crossroads". Monthly Forecast. (March 2026).

[272] Katharine Millar and Verónica Ferrari (2025). A Novel Approach to the 11 UN Norms for Responsible State Behaviour in Cyberspace: Guidelines for Gendered Implementation. Washington, DC: Organization of American States (OAS) and Geneva, Switzerland: UNIDIR; See also Report of the Secretary-General on Women and Peace and Security (28 September 2023) (S/2023/725); and UN Population Fund (UNFPA). "Technology-facilitated Gender-based Violence (TFGBV)".

[273] Informal Expert Group on Women and Peace and Security of the Security Council: Summary of the meeting on the situation in the Democratic Republic of the Congo, held on 6 November 2023 (6 December 2023) (S/2023/964).

[274] Security Council Meeting Record (6 October 2025) (S/PV.10011): annual open debate on women, peace and security; Report of the Secretary-General on Women and Peace and Security (28 September 2023) (S/2023/725).

[275] Report of the Secretary-General on Women and Peace and Security (5 September 2025) (S/2025/556); Report of the Secretary-General on Women and Peace and Security (25 September 2020) (S/2020/946): calling for a "gender data revolution" on WPS.

[276] Security Council Meeting Record (21 October 2024) (S/PV.9753): Council briefing on "Anticipating the impact of scientific developments on international peace and security" under the "maintenance of international peace and security" agenda item.

[277] Security Council Meeting Record (23 May 2022) (S/PV.9039): Council open briefing on Technology and security under the "maintenance of international peace and security" agenda item.

[278] Ibid.; See also UN Support Mission in Libya (UNSMIL) Press Release (16 January 2021). "ASRSG Williams conducts digital dialogue with 1000 Libyans".

[279] Informal Expert Group on Women and Peace and Security of the Security Council: Summary of the meeting on the situation in the Democratic Republic of the Congo, held on 6 November 2023 (6 December 2023) (S/2023/964).

[280] Informal Expert Group on Women and Peace and Security of the Security Council: Summary of the meeting on the situation in Yemen, held on 26 February 2024 (27 March 2024) (S/2024/269).

violence, illustrating how digital tools can be used to intimidate and silence women and other civic actors.[281]

These concerns have also appeared in preparatory documents for the Council's annual WPS debates. Switzerland's concept note for the 24 October 2024 open debate acknowledged that, while new technologies can create opportunities, including by enhancing women's participation, they also carry risks that can undermine such participation and access, particularly when women are targeted online in public and political spaces. It also included a guiding question on how new technologies could be used to promote women's participation in peace processes and protect women in the public sphere from threats, online harassment, and disinformation campaigns.[282]

Section V: Member State Dynamics on the Security Council's Role in Addressing ICTs and New and Emerging Technologies

The Security Council's engagement on ICTs and new and emerging technologies has unfolded against a backdrop of intensifying geopolitical competition, driven in part by the growing recognition that technological advantage in these areas is increasingly central to economic, military, and strategic power. In his 2023 report transmitting the work of the Advisory Board on Disarmament Matters, the Secretary-General conveyed the Board's warning that the pursuit and military use of emerging technologies in new domains, including cyberspace and AI, risked generating "arms-race-like dynamics".[283] The report also noted rising military spending and described the international security environment as marked by antagonistic interstate relations and hostile rhetoric, the resort to armed aggression in violation of international law, and mutual suspicion and trust deficits among states in many regions.[284]

This dynamic is also evident in the competition over the material inputs required for advanced technologies, including critical minerals and rare earths, which can create strategic dependencies and supply-chain vulnerabilities with potential peace and security implications.[285] These concerns were reflected in the Security Council briefing convened by the US on 5 March 2026 on "Energy, Critical Minerals, and Security" under the "Maintenance of international peace and security" agenda item.[286] In its concept note, the US argued that critical minerals and rare earths used in advanced technologies will become even more vital as AI, robotics, batteries, and autonomous devices transform economies, and warned that today's highly concentrated market could enable political coercion and supply-chain disruption. It also raised the question of how diversified, resilient, and secure critical minerals supply chains could be strengthened while advancing national security priorities.

These dynamics may complicate multilateral efforts to govern ICTs and new and emerging technologies, particularly in the military domain. The negotiations on the Pact of the Future offer one illustration of these challenges. Although the final text adopted at the Summit of the Future in September 2024 included a general commitment to seize the opportunities associated with new and emerging technologies and address the risks posed by their misuse, an earlier draft action point specifically addressing risks arising from the misuse of digital technologies, including ICTs and AI, was removed before adoption.[287]

Dynamics among Member States on the Council's Role in Addressing Cyber Threats

Member states have articulated differing views on the role of the Security Council in addressing cyber threats to international peace and security. Members advocating caution have emphasised the importance of respecting existing mandates and avoiding duplication of work undertaken in General Assembly processes. At the Council's June 2024 open debate on "Addressing evolving threats in cyberspace", for example, Egypt underscored that "inclusive processes within the [UN], primarily under the auspices of the General Assembly, are the most efficient way to establish equitable, comprehensive, and effective arrangements", and cautioned that the Council "should not be utilized as a legislative body that attempts to set norms and rules" on behalf of member states on matters that "necessarily require inclusive and transparent processes".[288]

China has expressed similar reservations. At a Council meeting on ransomware attacks against hospitals and other healthcare facilities and services, it described the issue as "highly specialized and technical" and suggested a preference for "more specialized, practical and

[281] Informal Expert Group on Women and Peace and Security of the Security Council, Summary of the meeting on the situation in Myanmar, held on 30 September 2024 (11 November 2024) (S/2024/813).

[282] Concept note for the annual Security Council open debate on women and peace and security, on the topic "Women building peace in a changing environment", to be held on Thursday, 24 October 2024 (3 October 2024) (S/2024/709); See also UN Women and Swiss Confederation (2024). Women Building Peace in a Changing Environment: Report of the Women Mediator Networks Retreat, Greentree, New York, held 17-19 July 2024.

[283] Report of the Secretary-General on Work of the Advisory Board on Disarmament Matters (31 July 2023) (A/78/287).

[284] Ibid., page 6.

[285] The Security Council has recognised the link between natural resources and conflict. See, for example, Statement by the President of the Security Council (25 June 2007) (S/PRST/2007/22).

[286] Security Council Report. "Briefing on Energy Critical Minerals and Security". What's in Blue. (4 March 2026).

[287] The deleted language would have reaffirmed the applicability of international law and the UN Charter to promoting a peaceful ICT environment; reaffirmed that voluntary, non-binding norms of responsible state behaviour in the use of ICTs can reduce risks to international peace, security and stability; called on states to refrain from ICT activity contrary to their obligations under international law that intentionally damages critical infrastructure; urged enhanced international cooperation and capacity-building to address threats arising from the misuse of digital technologies and close the digital divide; and called for the identification and addressing of risks associated with the military applications of AI across their lifecycle, in consultation with relevant stakeholders. Pact for the Future: Rev.4 (13 September 2024).

[288] Security Council Meeting Record (20 June 2024) (S/PV.9662).

in-depth discussions in other more appropriate platforms".[289] Brazil has similarly warned that "creating yet another forum for cyber discussions in the Council could work at cross-purposes with the goal of having a single, global track for the formulation and discussion of cyber norms and activities, diverting scarce resources and making it harder…to reach consensus in our debates". It nevertheless stressed that this does not preclude a role for the Council, which may be called upon to respond to "specific cyber incidents that have tangible impacts on peace and security and fall under its mandate".[290]

Russia has also taken a restrictive view of Council engagement on cyber issues. It has argued that "duplicating the efforts of the international community and spreading this topic across various [UN] platforms is counterproductive and could nullify all the results achieved over decades under the auspices of the General Assembly".[291] In its view, cyber issues should remain primarily within General Assembly processes because the subject "has its own specifics and should be discussed at specialized platforms holding relevant expertise". Russia has also stressed the inclusivity of the OEWG, noting that it includes all UN member states on an equal footing and operates by consensus. More broadly, Russia has stated that it does "not support the call to raise awareness of the international community on the issues of [international information security] through the convening of regular meetings of the Security Council". Russia has also linked its caution to attribution challenges, arguing that threats in the information space are "extremely difficult to identify", including their source, and warning that "[u]ntil the problem of attribution is resolved", discussion in the Council "may turn into another exchange of unsubstantiated allegations.[292]

By contrast, proponents of stronger Council engagement have argued that the link between cyber threats and international peace and security is clear. In their view, malicious cyber activities can aggravate existing conflicts and affect the implementation of the Council's existing work, including with regards to sanctions regimes and peacekeeping mandates. They have therefore called for a more "comprehensive, responsive, and evidence-based approach" if the Council is to remain agile and relevant in the face of rapid technological change.[293]

These members have proposed several avenues for stronger Council engagement on cyber-related threats, including regular briefings and periodic reporting by the Secretary-General on developments in the cyber threat landscape and their implications for international peace and security, as well as the mainstreaming of cyber-related concerns across country-specific and thematic agenda items, with at least one Council member suggesting that it consider incorporating "cybersecurity-related elements" into its products "according to the needs of each dossier".[294] Some have also highlighted the potential relevance of Council engagement in cases involving large-scale cyber incidents. One member state, for example, pointed to Article 34 of the Charter as a basis for Security Council investigations of situations that might lead to international friction or give rise to a dispute, arguing that, given the full applicability of the Charter to the use of ICTs by states, the Council's dispute-settlement role under Chapter VI is also relevant in this context.[295]

At the same time, these members have stressed that any Council role should reinforce and complement, rather than duplicate, the ongoing work of the General Assembly. In their view, while norm-setting and rule development should continue to be pursued through inclusive, state-led processes in the General Assembly, the Council can contribute by monitoring evolving threats, integrating cyber-related considerations into its existing work, and reinforcing the existing framework of responsible state behaviour.

Toward a Complementary Division of Labour between the Security Council and the General Assembly

The Security Council and the General Assembly are often seen as having distinct strengths and limitations. General Assembly processes have served as the intergovernmental forum for developing and elaborating the UN framework of responsible state behaviour in the use of ICTs, and their more inclusive character in recent years has further strengthened their political legitimacy. These processes have yielded important achievements, including the affirmation that existing international law, in particular the UN Charter, applies to the use of ICTs by states; the articulation of the eleven voluntary, non-binding norms of responsible state behaviour in cyberspace; and agreement on important confidence-building measures, including the creation in 2022 of the global intergovernmental Points of Contact Directory.[296] Capacity-building has also become a central pillar of General Assembly processes. OEWG reports have repeatedly stressed the need for sustainable, effective, and affordable solutions,

[289] Security Council Meeting Record (8 November 2024) (S/PV.9779).

[290] Presentations and Statements made at the UN Security Council Arria-formula Meeting on "The responsibility and responsiveness of States to cyberattacks on critical infrastructure", held on 25 May 2023 (7 June 2023) (S/2023/412).

[291] Permanent Mission of the Russian Federation to the UN. "Statement by Permanent Representative Vassily Nebenzia at UNSC open debate 'Addressing evolving threats in cyberspace'" (20 June 2024).

[292] Ibid.

[293] Joint Statement on the Use of Information and Communications Technology in the Context of International Peace and Security, delivered by the Republic of Korea at the Security Council open debate on 20 June 2024 on behalf of 63 member states and the European Union, including France, the United Kingdom, and the United States.

[294] See, for example, the remarks by the Republic of Korea at the Security Council high-level open debate on "Addressing evolving threats in cyberspace" (20 June 2024) (S/PV.9662): stating that the Council can "request a report on a regular basis to consider how cyber threats intersect with the Council's mandate, and how evolving cyber threats impact international peace and security"; the statement by the United Arab Emirates (UAE) at the same Security Council open debate (20 June 2024) (S/PV.9662): suggesting that "the publication of an annual cybersecurity report by the Secretary-General will provide a comprehensive assessment of the global cyber threat landscape and recommendations for enhancing international cooperation. This should also include gender analysis to better respond to threats in cyberspace targeting women and girls"; the statement by Slovenia at the briefing on ransomware attacks against hospitals and other healthcare facilities and services (8 November 2024) (S/PV.9779): suggested that the Council consider listing "cybercriminals" under relevant sanctions regimes; and the statement by Ecuador at the Security Council open debate on "Addressing evolving threats in cyberspace" (20 June 2024) (S/PV.9662).

[295] Germany, for example, suggested at the 20 June 2024 open debate (S/PV.9662) that the Council could play a "strong trust- and norm-building role" by placing international cyber conflicts on its agenda, investigating situations of cyber conflict, or facilitating their peaceful settlement, thereby contributing to the evolving framework of responsible state behaviour in cyberspace; Similarly, the joint statement delivered ahead of the open debate by the Republic of Korea on behalf of 63 member states and the European Union stressed that the Council's role in cybersecurity "must reinforce and complement the existing and ongoing work of the General Assembly", while recognising "the importance of the Council's reaffirmation of the UN framework of responsible State behaviour in the use of ICTs".

[296] Launched in 2024, the Directory is intended to facilitate secure and direct communication between states to help prevent and address serious ICT incidents and de-escalate tensions in crises, including incidents affecting critical infrastructure with national, regional, or global impact. As at 15 October 2025, more than 120 countries had joined the Directory and nominated national points of contact, indicating substantial engagement. See Second Annual Progress Report of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021-2025 (1 August 2023) (A/78/265), annex A; UNIDIR (15 October 2025). UNIDIR Event on "Advancing the UN Global Intergovernmental Points of Contact Directory: Smooth transition and further development", New York: United Nations; and UNODA. "Welcome to the Global Intergovernmental Points of Contact Directory on the Use of Information and Communications Technologies in the Context of International Security".

particularly for developing countries, and have linked needs-based capacity-building to stronger resilience, improved ICT security, and efforts to bridge digital divides.[297]

The Security Council, by contrast, has primary responsibility under the UN Charter for the maintenance of international peace and security and may adopt binding decisions under Chapter VII. It also has several tools, including sanctions regimes and peace operations, through which agreed normative understandings may be incorporated into mandates and measures tailored to specific country situations. Both bodies, however, face structural constraints. Consensus-based decision-making in the General Assembly can produce lowest-common-denominator outcomes and may also require prolonged negotiations before agreement is reached, while Security Council resolutions on substantive matters may be blocked by the veto of a permanent member, and presidential statements and press statements require consensus.

Divisions are evident, even among proponents of stronger Council engagement, over what a division of labour between the Security Council and the General Assembly should look like in practice. Some member states have suggested that the Security Council may be well placed to examine specific cyber-related disputes or situations that could endanger international peace and security. Where cyber incidents rise to that level, they argue, the Council could contribute to de-escalation, including through its investigative and dispute settlement functions under Chapter VI and, where appropriate, its more coercive tools under Chapter VII.[298]

Some have also suggested that, while the Council may be well placed to promote adherence to agreed norms through its operational tools, the development of new norms should remain within the purview of the General Assembly and its mandated expert processes.[299] At least one member state, however, has explicitly suggested a norm-setting role for the Council.[300] Other members have offered ideas on how to bridge the work of the two bodies. One Council member suggested the Council consider the findings of the Secretary-General's reports to the General Assembly on developments in the field of ICTs in the context of international security, while a member state highlighted an example of a commission issuing recommendations directly to the Security Council, which it said could provide states with concrete tools for implementation.[301] Russia, by contrast, has objected more broadly to Council engagement on this issue, indicating that any workable understanding of complementarity is likely to emerge only gradually through institutional practice. At the same time, member states have given only limited consideration to how such complementarity might operate in practice, suggesting that the issue remains underexplored and would benefit from further reflection.

Case Study: Small Arms and Light Weapons as a Model of General Assembly–Security Council Complementarity

The evolution of UN engagement on small arms and light weapons (SALW) may offer a useful point of comparison for ongoing debates about the respective roles of the General Assembly, intergovernmental processes linked to it, and the Security Council in addressing cyber threats. Although the two issue areas are not directly analogous, the SALW agenda shows how a complementary relationship between the General Assembly and the Security Council can emerge gradually over time..

By decision 55/415 (2000), the General Assembly agreed to convene the UN Conference on the Illicit Trade in Small Arms and Light Weapons in All Its Aspects.[302] At the conference, held in July 2001, member states adopted the Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in SALW in All Its Aspects (PoA), through which governments committed to strengthening national small arms regulations, stockpile management, weapons marking and tracing, and regional and international cooperation and assistance.[303] The PoA also included global commitments to cooperate with the UN system in implementing Security Council arms embargoes and to encourage the Council to consider including relevant provisions on disarmament, demobilisation, and reintegration (DDR) in peacekeeping mandates.[304] The PoA remains the central framework for global efforts to address the impact of SALW, guide national regulation, strengthen international cooperation, and support capacity-building to combat the illicit trade and misuse of these weapons.[305]

The Security Council, for its part, first considered SALW as a standalone thematic issue in 1999, when the Netherlands convened a ministerial debate under the heading "Small arms", thereby establishing it as a formal agenda item.[306] The Council's engagement on SALW has, however, been uneven. Although it adopted six presidential statements on small arms between 1999 and 2007, the issue was largely absent from the Council's agenda for several years thereafter.[307] The Council adopted its first thematic resolution on SALW in September 2013, fourteen years after first

[297] Final Report of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021-2025 (24 July 2025) (A/80/257).

[298] Official Compendium of Voluntary National Contributions on the subject of how International Law applies to the Use of Information and Communications Technologies by States (13 July 2021) (A/76/136): Australia's position: stating that the Security Council may exercise its powers and responsibilities under Chapters VI and VII of the Charter with respect to cyber activities endangering international peace and security, and that resolution of a cyber dispute under Chapter VI could include referral to the International Court of Justice; Estonia's position: stating that under Chapter VI the Council may call upon parties to settle their dispute by peaceful means and that, in specific cases involving cyber activities endangering international peace and security, the Council's other Charter powers and responsibilities may be exercised; and Japan's position: stating that, in order to ensure the peaceful settlement of disputes, the Council's powers under Chapters VI and VII and the functions of other UN organs, including the International Court of Justice, should be used in disputes stemming from cyber operations; and Statement by Tobias Lindner, Minister of State at the German Federal Foreign Office at the Security Council high-level open debate on "Addressing evolving threats in cyberspace" (20 June 2024) (S/PV.9662): stating that the Council has an important role in assessing the threat, including under Article 34 of the Charter, and should consider more deeply the risks emanating from cyberattacks for international peace and security.

[299] Statement by Switzerland at the same Security Council open debate (20 June 2024) (S/PV.9662): "It is not for the Council to develop rules of behaviour or agreements. That is the prerogative of the General Assembly and the expert processes it has mandated"; Statement by Brazil in the annex to the letter dated 7 June 2023 from the Permanent Representative of the United States of America to the United Nations addressed to the Secretary-General, S/2023/412: warning that creating "yet another forum for cyber discussions in the Council" could undermine "a single, global track for the formulation and discussion of cyber norms and activities", and stressing that the General Assembly "has been able to take concrete steps, including defining, by consensus, norms of responsible state behaviour".

[300] Statement by Mozambique at the 20 June 2024 Security Council open debate (S/PV.9662).

[301] See Slovenia's statement at the 20 June 2024 Security Council open debate (S/PV.9662 (Resumption I); and Mexico's Statement regarding the OEWG Chair's Draft Elements for the Open-Ended Action-Oriented Permanent Mechanism on ICT Security in the Context of International Security" (17 May 2024): cited the International Law Commission as an example of a commission issuing recommendations directly to the Security Council or the General Assembly.

[302] General Assembly Decision on Small Arms (20 November 2000) (A/DEC/55/415).

[303] UNODA. "Small Arms and Light Weapons".

[304] Report of the United Nations Conference on the Illicit Trade in Small Arms and Light Weapons in All Its Aspects (20 July 2001) (A/CONF.192/15), annex

[305] UNODA, Regional Centre for Peace and Disarmament in Asia and the Pacific. "Programme of Action".

[306] Security Council Meeting Record (24 September 1999) (S/PV.4048).

[307] The Security Council did not convene a debate to discuss the Secretary-General's 2011 Report on Small Arms (5 April 2011) (S/2011/255). Instead, it organised a briefing in a closed meeting; See Security Council Report. "Small Arms". Monthly Forecast. (May 2015).

considering the issue as a standalone item, followed by further thematic resolutions in May 2015 and December 2021.[308]

Despite this uneven thematic engagement, the Council has been able to operationalise the SALW agenda in the situations on its agenda, most notably through arms embargoes and related sanctions provisions.[309] These have included prohibitions on the supply of arms, ammunition, military materiel, and related assistance to a state, territory, or named party.[310] The Council has also established sanctions committees and panels or groups of experts to investigate violations, identify supply routes, and recommend ways to strengthen implementation. In some cases, it has linked embargo violations to targeted measures such as travel bans and asset freezes.[311] In certain settings, it has further mandated UN peace operations to support the monitoring of embargo implementation or related weapons and ammunition management tasks.[312]

The Council has also addressed the threats posed by SALW through disarmament-related measures in conflict and post-conflict settings. It has supported DDR processes in peace agreements and ceasefire contexts, and has mandated multidimensional peace operations to assist with DDR, security sector reform (SSR), police reform, the restructuring of armed forces, and weapons and ammunition management. Over time, DDR and related SSR tasks became recurring features of Council mandates in a number of settings, including Sierra Leone, Liberia, Haiti, Côte d'Ivoire, the DRC, and the CAR.[313]

This division of labour has allowed the General Assembly and the Security Council to perform distinct but mutually reinforcing functions. General Assembly-led processes, including the PoA and the International Tracing Instrument, have provided the core normative, policy, and capacity-building framework for addressing SALW. The Council, for its part, has addressed the issue both as a standalone agenda item and through its integration into decisions and discussions on relevant thematic issues and country situations.[314]

The SALW experience may offer a useful point of comparison for cyber threats. Rather than serving as a forum for cyber governance or norm-elaboration, the Council could gradually define its role by integrating cyber-related risks into existing country-specific and thematic files where those risks exacerbate armed conflict, undermine peace operations, facilitate sanctions evasion, raise civilian protection concerns, or otherwise threaten international peace and security. At the same time, some of the political and institutional sensitivities visible in current cyber discussions, including concerns about the scope of the Council's role, were also present in its early engagement on SALW.[315] Over time, however, incremental engagement, normative consolidation, and practical necessity helped make SALW a more regular feature of the Council's work.

Dynamics among Member States on the Council's Role in Addressing AI and New and Emerging Technologies

AI, and new and emerging technologies more broadly, are relatively new thematic issues for both the Security Council and the wider UN system. There is no long-standing intergovernmental process dedicated to their peace and security implications.[316] This stands in contrast to ICTs, which have been on the General Assembly's agenda since 1998 and discussed in intergovernmental processes since 2004. Many of these technologies are also still evolving, with effects that may prove transformative, while their growing convergence creates new combinations of risks and opportunities. As a result, an understanding of how they relate to international peace and security is still developing, and member states' positions are still taking shape, both regarding their implications and the role the Council should play in addressing them.

Nevertheless, a substantial number of member states consider the link between these technologies, particularly AI, and international peace and security sufficiently clear to warrant more sustained Council attention. For these states, the priority is to ensure that the Council is better positioned to anticipate, assess, and respond to emerging risks in this domain.[317] In practical terms, this has led some to call for more regular Secretariat briefings and reporting by the Secretary-General on the evolving threat landscape and on the ways in which these technologies may affect the Council's work.[318] Others have envisaged a more direct role for the Council in situations where AI materially shapes conflict dynamics,

[308] Security Council Resolution 2117 (26 September 2013) (S/RES/2117); Security Council Resolution 2220 (22 May 2015) (S/RES/2220); Security Council Resolution 2616 (22 December 2021) (S/RES/2616).

[309] Security Council Report. Cross-Cutting Report No. 3: The Security Council's Role in Disarmament and Arms Control: Conventional Weapons and Small Arms (24 September 2009).

[310] For examples of arms embargoes, see Security Council Resolution 1171 (5 June 1998) (S/RES/1171); Security Council Resolution 1493 (28 July 2003) (S/RES/1493); and Security Council resolution 2127 (5 December 2013) (S/RES/2127).

[311] For monitoring architecture, see Security Council Resolution 1533 (12 March 2004) (S/RES/1533); For targeted sanctions linked to embargo breaches, see Security Council Resolution 2262 (27 January 2016) (S/RES/2262).

[312] For peace operations supporting implementation, see Security Council Resolution 2149 (10 April 2014) (S/RES/2149); and Security Council Resolution 2605 (12 November 2021) (S/RES/2605).

[313] For Sierra Leone, see Security Council Resolution 1270 (22 October 1999) (S/RES/1270); for Liberia, see Security Council Resolution 1509 (2003), S/RES/1509 (19 September 2003); for Haiti, see Security Council Resolution 1542 (30 April 2004) (S/RES/1542); for Côte d'Ivoire, see Security Council Resolution 1609 (24 June 2005) (S/RES/1609); for the DRC, see Security Council Resolution 2098 (28 March 2013) (S/RES/2098); and for CAR, see Security Council Resolution 2149 (10 April 2014) (S/RES/2149).

[314] Report of the Secretary-General on Assistance to States for curbing the illicit traffic in small arms and light weapons and collecting them and the illicit trade in small arms and light weapons in all its aspects (17 June 2025) (A/80/111).

[315] See Chapter VIII, Section 44: "Small arms" in Repertoire of the Practice of the Security Council, 1996–1999. (2009) (ST/PSCA/1/Add.13).

[316] See General Assembly Resolution 43/77 (7 December 1988) (A/RES/43/77), which first placed "Scientific and technological developments and their impact on international security" on the Assembly's agenda, and resolutions 72/28 (2017) and 78/22 (2023), under which the Secretary-General has submitted reports on current developments in science and technology and their potential impact on international security and disarmament, but without an accompanying standing intergovernmental dialogue process; General Assembly Resolution 79/239 (24 December 2024) (A/RES/79/239) on "artificial intelligence in the military domain and its implications for international peace and security", indicating that discussion of AI in the military domain remains at an early stage; The Pact for the Future (22 September 2024) (A/RES/79/1), which launched the Independent International Scientific Panel on AI and the Global Dialogue on AI Governance in the non-military domain; the OHCHR Mapping Report on Human Rights and New and Emerging Digital Technologies (20 August 2024) (A/HRC/56/45), which addresses technologies including neurotechnology; and the work of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems under the Convention on Certain Conventional Weapons.

[317] See, for example, Joint Statement by current and former Council members Denmark, Greece, France, and Slovenia on Artificial Intelligence and International Peace and Security (31 December 2025): recognising the transformative potential of AI for international peace and security as well as the significant risks arising from its irresponsible use; noting that the misuse of AI may exacerbate existing conflicts, shape their dynamics, and pose additional threats to international peace and security; emphasising that the rapid development and deployment of AI can both support and challenge the Security Council's deliberations and mandates; and, in that regard, urging Council members and other stakeholders to collaborate closely to anticipate, assess and address emerging risks.

[318] Security Council Meeting Record (24-25 September 2025) (S/PV.10005 and S/PV.10005 (Resumption I)): see Slovenia calling for regular briefings by the Secretary-General on developments in AI affecting international peace and security and for the inclusion of AI-related risks on the Council's agenda; and Somalia urging regular monitoring and assessment of emerging AI threats, the sharing of best practices, and investment in early-warning systems. See also Security Council Meeting Record (21 October 2024) (S/PV.9753): Mozambique states that the Council needs to hold regular briefings and produce reports for the benefit of the entire international community on the latest scientific advancements and their possible impacts on peace and security; and See also Security Council Meeting Record (19 December 2024) (S/PV.9821): Slovenia advocates for the integration of AI-related discussions into the Council, including through briefings to ensure that members pay attention and provide responses to those risks within existing Council mandates and other geographic and thematic issues.

arguing that it could help coordinate international responses to conflicts catalysed or intensified by AI.[319]

Beyond monitoring and assessment, some member states have argued that the Council can serve as a useful forum for promoting responsible approaches to AI and facilitating the exchange of experience and good practices. Advocates of this view believe that the Council can help encourage compliance with international law, reinforce the importance of meaningful human oversight and the retention of human agency in military applications, and support broader normative and policy discussions on the peace and security implications of these technologies.[320]

A related strand of thinking focuses less on AI as an object of Council discussion in its own right and more on how these technologies may affect, and potentially support, the Council's existing work. Some member states have suggested that the Council should make better use of technological developments in areas such as early warning, conflict analysis, risk assessment, humanitarian coordination, ceasefire verification, and the protection of civilians and UN personnel. Others have emphasised the need to strengthen missions' capacity to address AI-enabled threats, including online disinformation and misinformation, as well as cyberattacks.[321] In the non-proliferation context, one member state has further suggested that the Council consider an approach analogous to resolution 1540 (2004) in relation to AI capabilities in the hands of non-state actors.[322]

Not all member states, however, favour a broader Council role. One group has expressed caution about expanding Council engagement on AI. Russia, for example, has questioned whether AI, as a broad thematic issue, falls clearly within the Council's mandate and has argued that such discussions should instead take place in broader and more inclusive multilateral forums.[323] Others have stressed that any Council engagement should remain complementary to wider UN processes and specialised discussions on technological governance and the military dimensions of AI.[324] Brazil, for example, has argued that while the Council should remain vigilant and ready to respond to incidents involving the use of AI, the international community should be careful not to over-securitise the issue by concentrating discussion in the Council.[325] For some states, including the US, these reservations also reflect broader positions on AI governance, including opposition to more centralised international approaches.

These differences are borne out in the Council's own practice. The presidential statement adopted in October 2024 on the impact of scientific developments on international peace and security was the Council's first product specifically focused on technology and peace and security.[326] It recognised that the convergence of scientific fields may accelerate technological capabilities in ways that carry both opportunities and risks for international peace and security and for the Council's own work. It also expressed the Council's continued commitment to take scientific advances into account more systematically, where appropriate and in line with its mandate, insofar as they affect international peace and security.

Yet the negotiation of that text also revealed the current limits of consensus. Earlier drafts apparently included more operational provisions, including language encouraging the Secretary-General, where appropriate, to reflect scientific advances in reporting on situations on the Council's agenda, as well as references to expert advice and partnerships with scientific actors to support the Council with evidence-based information. These elements were ultimately removed from the text adopted by the Council. A reference to the need to anticipate, in addition to taking into account, the impact of scientific developments was also dropped, weakening the text's preventive thrust. This suggests that, while member states may be prepared to endorse broad language in principle, they remain more hesitant about formulations that could carry concrete operational implications for the Council's work.

The same dynamic is likely to continue to shape future efforts to secure a Council product specifically on AI. At present, member states appear more able to agree on general language acknowledging the relevance of technological change to international peace and security than on steps that would operationalise that recognition in the Council's day-to-day work. Still, the discussion to date points to a growing recognition that AI and other new and emerging technologies have implications for international peace and security that the Council cannot ignore indefinitely. The issue, for now, is less whether the Council should engage at all than how far, and in what ways, that engagement can be made more practical without provoking criticism over mandate expansion or duplication of work elsewhere in the UN system.

[319] Security Council Meeting Record (25 September 2025) (S/PV.10005 (Resumption I)): see Singapore stating that the Council could have a role in coordinating international responses in situations "turbo-charged and catalysed by AI".

[320] Ibid., see Sierra Leone stating that the Council can encourage best practices in peace operations, promote safeguards to retain human agency in military uses, and ensure compliance with international law and international humanitarian law; Mexico supporting meaningful human oversight and accountability mechanisms, including prior reviews under article 36 of Additional Protocol I; Somalia calling for clear global standards for the responsible use of AI; China calling for ethical norms and accountability mechanisms.

[321] Ibid., see Ecuador calling for the systematic integration of technological considerations into prevention, peacekeeping and peacebuilding; Guyana suggesting the use of AI tools to identify signs of possible conflict, monitor misinformation and disinformation, assess risks in peacekeeping operations, improve sanctions implementation and track ceasefire violations; Portugal proposing practical measures such as equipping missions to confront disinformation campaigns and using AI tools to improve risk prevention and analysis; Burundi advocating the integration of an AI dimension into conflict analysis and peace operation mandates; Denmark highlighting AI's potential for sanctions monitoring, countering misinformation and remote ceasefire monitoring; and China urging the Council to give due priority to the risks posed by the misuse of AI by terrorist groups, extremist forces and transnational criminal networks.

[322] Ibid., see Morocco suggesting that, with respect to AI capabilities in the hands of non-State actors and terrorist groups, the Council could consider an approach similar to resolution 1540 (2004).

[323] Security Council Meeting Record (24 September 2025) (S/PV.10005).

[324] Security Council Meeting Record (24-25 September 2025) (S/PV.10005 and S/PV.10005 (Resumption I): see Sierra Leone and France stressing that any Council role should remain complementary to wider UN efforts and other ongoing processes.

[325] Security Council Meeting Record (18 July 2023) (S/PV.9381).

[326] Statement by the President of the Security Council (21 October 2024) (S/PRST/2024/6).

Section VI: Options for Security Council Engagement on ICTs and New and Emerging Technologies

Divergent views among member states on the role of the Security Council in addressing issues related to ICTs and new and emerging technologies, including AI, have so far constrained the scope for stronger Council engagement. At the same time, there is growing recognition that, as these technologies expand in scale and complexity, their implications for the maintenance of international peace and security are likely to become more pronounced.

Without more systematic attention, the risks associated with technological change may outpace the Council's capacity to respond effectively. To address the peace and security implications of these developments, the Council will need to strengthen its engagement on the issues within its mandate that are shaped by technological developments. Although current dynamics may make it difficult to adopt a formal product on ICTs or AI, Council members nevertheless have a range of tools they can use to address these issues more systematically, consistent with the commitment expressed in the Council's 21 October 2024 presidential statement on the impacts of scientific developments on peace and security.[327] Other stakeholders also have tools available to support the Council's work in this area.

This section sets out practical options for strengthening the Council's engagement on ICTs and new and emerging technologies. The recommendations build on existing practice, working methods, and precedents, and are organised by stakeholder: Council members, non-Council members and the wider UN membership, the UN Secretariat, and non-governmental organisations and private sector actors.

Options for Security Council Members

Recommendation 1: Establish an Informal Expert Group on Technology, Peace and Security

A low-threshold option for the Council would be to establish an informal expert group (IEG) on technology, peace and security. Such a group could bring together Council members at the expert level for systematic and timely consultations on issues related to ICTs, AI, and other new and emerging technologies. Its establishment would not require a formal Council product, such as a resolution or presidential statement, or full consensus among Council members. Rather, it could be initiated by one or more interested members with broad support from others.

There is precedent for this approach. The IEG on the Protection of Civilians was created in 2009 at the initiative of the UK, following a recommendation by the Secretary-General, without a formal Council product.[328] Similarly, the Informal Expert Group of members of the Security Council on Climate, Peace and Security was launched in 2020 through an initiative led by Germany and other Council members, also without a formal Council product.

The experience of the IEG on the Protection of Civilians illustrates the potential value of such a forum. Since its first meeting in January 2009, the group has convened regularly, primarily in connection with mandate renewals, to receive briefings from the UN Office for the Coordination of Humanitarian Affairs (OCHA) and other UN entities, identify key protection concerns, and consider possible options for Council action.[329] These meetings are not used to negotiate outcomes. Rather, they provide Council members with useful information for upcoming mandate discussions and negotiations. Over time, the group has helped support the more systematic integration of protection considerations into Council products.

An IEG on technology, peace and security could serve a similar function. It could provide a structured space for Council members to consider both how threats arising from the malicious use of ICTs, AI, and other new and emerging technologies, including through their convergence, relate to country situations and thematic issues on the Council's agenda, as well as how these technologies might be used to strengthen the Council's work, including in the context of peace operations and sanctions. Meetings could be held ahead of mandate renewals where such issues are particularly salient, or convened in response to significant technology-related incidents affecting international peace and security or the Council's own work. Over time, this could support more systematic consideration of the peace and security implications of technology across the Council's activities.

The group could also convene thematic meetings to support horizon scanning and early warning, thereby helping to operationalise the Council's commitment to "take into account scientific advances more systematically".[330] Such discussions could focus on cross-cutting issues, such as malicious cyber activity affecting UN missions or the implementation of sanctions regimes. They could also take a more forward-looking approach, addressing risks associated with the military application of emerging technologies, including quantum computing, neurotechnology, and advanced robotics—areas that have so far received limited attention in Council deliberations.

An IEG on technology, peace and security could draw on expertise from across the UN system, including UNODA, OICT, the UN Institute for Disarmament Research (UNIDIR), CTED, UNOCT, peace operations, and panels of experts of sanctions regimes, as well as external civil society representatives and private sector actors. In this way, it could help bring together analysis that is currently dispersed across institutional silos. UNODA could play a coordinating role for such meetings, comparable in some respects to that played by OCHA in support of the IEG on the Protection of Civilians. In preparing discussions, it could also draw on expertise from across the UN system through existing inter-agency mechanisms, including the UN Cyber Hub, which allows UN entities to exchange substantive updates on cyber-related work and identify synergies across departments and agencies.[331]

An informal group would have both limitations and advantages. Participation would be voluntary, and discussions would not reflect Council consensus. However, flexibility in convening, agenda-setting, and participation would lower political barriers and allow engagement even in the absence of unanimity. As in some other IEGs,

[327] Adoption of a draft resolution on a substantive matter requires an affirmative vote of at least nine Council members and no negative vote by a permanent member. Presidential statements are adopted by consensus.

[328] Report of the Secretary-General on the Protection of Civilians in Armed Conflict (28 October 2007) (S/2007/643).

[329] A comparable practice exists in the context of the Informal Expert Group on Women, Peace and Security, which was established by resolution 2242 (2015) and meets in connection with country situations on the Council's agenda.

[330] Statement by the President of the Security Council (21 October 2024) (S/PRST/2024/6).

[331] Internet Governance Forum (IGF). "IGF Engagement within the UN System".

chairs could circulate an informal summary for internal use, without requiring consensus, to set out key issues and options without attributing positions.

In practical terms, the group could be established incrementally. One or more Council members could propose its creation, consult with other members, and indicate their willingness to serve as chair or co-chairs of the IEG. They could also make clear that the initiative would be without prejudice to General Assembly-led processes, including the newly established permanent Global Mechanism on developments in the field of ICTs in the context of international security and advancing responsible State behaviour in the use of ICTs.[332]

The case for such a group is that the Council currently lacks a mechanism with the expertise and analytical depth needed to address the peace and security implications of technological developments in an integrated manner. These risks do not always map neatly onto specific items on the Council's agenda. A cyber incident affecting critical energy infrastructure, for example, may simultaneously raise PoC concerns, implicate sanctions compliance, involve terrorist groups, and affect the operational environment of peacekeeping or political missions. Existing informal expert groups and subsidiary bodies tend to address only particular aspects of such incidents within their respective mandates, rather than offering a cross-cutting assessment. Nor is the technical expertise needed to analyse such risks systematically embedded in the Council's existing tools. An IEG on technology, peace and security could help fill these gaps by consolidating analysis across domains, identifying where technological developments alter risk profiles or mandate requirements, and equipping Council members with coherent, context-specific insights ahead of mandate renewals, without creating new reporting obligations or duplicating General Assembly-led processes.

A broader remit covering ICTs alongside new and emerging technologies, including AI, would reflect the extent to which the risks associated with these technologies increasingly converge in practice. It would also help ensure that the group is not tied too narrowly to specific technologies that may quickly be overtaken by scientific and technological developments, allowing it to maintain a more adaptable and forward-looking focus on the operational implications of technological change for Council mandates and decision-making. More broadly, this framing would help avoid reproducing within the Council the compartmentalisation that characterises wider UN discussions on technology, which remain spread across several intergovernmental processes. Rather than creating another technology-specific silo, such a forum could provide a space to connect these parallel discussions and enable members to consider how developments across domains interact in concrete peace and security contexts.

Recommendation 2: Establish a Voluntary Commitments Initiative to Encourage More Systematic Consideration of ICTs and New and Emerging Technologies in Security Council Practice

A complementary option for strengthening the Council's engagement on ICTs, AI, and other new and emerging technologies would be to launch a voluntary political initiative based on shared commitments among a small group of Council members. Such an initiative would not require a formal Council product, but would instead depend on political will, coordination, and sustained practice. There is precedent for this approach in the Women, Peace and Security (WPS) Shared Commitments initiative and the Climate, Peace and Security pledges, which show how coordinated political leadership, including through consecutive presidencies, can help embed a cross-cutting issue more systematically in the Council's day-to-day work without reopening normative debates or creating new mandates.

Case Study: The Women, Peace and Security Shared Commitments

The WPS Shared Commitments were first articulated on 31 August 2021, when Ireland circulated a joint Statement of Shared Commitments on WPS drafted with Kenya and Mexico. The three members pledged to make WPS a priority during their consecutive presidencies, with the stated aim of narrowing the gap between rhetorical support for the agenda and its practical implementation. The initiative was framed as a "golden thread" running through their presidencies and focused on integrating WPS considerations more systematically into Council discussions and products.[333] It was not intended to introduce new norms, but rather to operationalise existing commitments through practical, implementation-focused measures.

The initiative later expanded beyond the original trio. A second Statement of Shared Commitments, issued on 1 December 2021 by Albania, Niger, Norway, and the United Arab Emirates, allowed other Council members to associate themselves with the initiative.[334] More than 20 current and former Council members, including permanent members, have endorsed the shared commitments, illustrating how an informal political pledge can evolve into a more durable practice.[335]

The WPS commitments initiative highlights several features that could be adapted to the peace and security implications of technology. First, it began with a small group of like-minded members but was designed in a way that allowed broader uptake over time. Second, the initiative focused on integration, committing members to reflect WPS considerations in country-specific mandates, thematic debates, and routine Council business. Third, it relied on continuity and visibility, including through consecutive presidencies, signature events, and efforts to carry forward lessons and good practices across presidencies. This sort of initiative, however, is dependent on the political will and creativity of its participating members.[336]

A similar initiative could be developed on ICTs and new and

[332] The Global Mechanism emerged from the 2021-2025 Open-Ended Working Group process and is intended to serve, from 2026, as a permanent, action-oriented framework for continued discussions on ICTs in the context of international security and advancing responsible state behaviour. See UN General Assembly Draft Resolution, authored by Singapore (13 October 2025) (A/C.1/80/L.20); and UNIDIR. UNIDIR Event on "Engaging Regions: Insights into the Global Mechanism on ICT Security", held on 26-27 November 2025.

[333] During the press conference on the Security Council's programme of work for September 2021, Ambassador Geraldine Byrne Nason of Ireland described the initiative as "a golden thread" running through the Irish, Kenyan, and Mexican presidencies. See Security Council Report. "Golden Threads and Persisting Challenges: The Security Council Women, Peace and Security Presidencies Initiative". 2022, No.3 Report. (30 December 2022); and Security Council Report. "In Hindsight: Women, Peace and Security, Golden Threads and Persisting Challenges". Monthly Forecast. (December 2021).

[334] Security Council Report. "Women, Peace and Security: One Year of Shared Commitments". Monthly Forecast. (December 2022).

[335] NGO Working Group on Women, Peace and Security Home webpage.

[336] For example, implementation of the WPS Shared Commitments has been uneven, with some commitments receiving only limited proactive and substantive follow-through. Recent continuity has also often taken the form of regular strategy meetings and joint press stakeouts rather than more systematic integration across Council practice. See Security Council Report. "Women, Peace and Security: One Year of Shared Commitments". Monthly Forecast. (December 2022).

emerging technologies. Interested Council members could agree on a set of shared political commitments aimed at treating these issues more consistently as cross-cutting dimensions of the Council's responsibility for maintaining international peace and security. As with the WPS precedent, the aim would not be to create new structures or reporting requirements, but to encourage more systematic consideration of technological risks and opportunities across the Council's existing work.

In practice, such a voluntary initiative could include commitments to:

- coordinate across participating presidencies to convene annual open debates on the impacts of ICTs, AI, and other new and emerging technologies on international peace and security, with a view to raising awareness of evolving risks;
- ensure that technological dimensions are addressed, where relevant, in country-specific discussions on the Council's agenda;
- ensure that signature events during participating members' presidencies include substantive analysis of the technological dimensions relevant to the issues under discussion;
- convene meetings, where appropriate, on significant cyber incidents, consistent with Article 34 of the Charter, either in a formal format where sufficient support exists or through informal formats where sensitivities persist;
- encourage UN briefers to include analysis of technological risks and opportunities, including their gendered impacts and their implications for the rights, participation, and protection of women and girls, as well as for conflict dynamics, civilian harm, humanitarian access, sanctions implementation, and mandate delivery, and raise these issues in Council members' questions to Secretariat briefers during consultations;
- enhance the visibility of the Council's engagement on ICTs, AI, and other new and emerging technologies through joint press stakeouts and presidency press briefings;
- promote the inclusion of relevant language in Council statements and other products, including reaffirmations of existing norms of responsible state behaviour in the use of ICTs and confidence-building measures such as the Point of Contact Directory, thereby reinforcing complementarity with General Assembly-led processes, including the new Global Mechanism;
- ensure that products drafted by participating members reflect the technological dimensions of the issues under consideration, drawing on analysis and guidance generated through a potential informal expert group on technology, peace and security;
- prepare a short handover note at the end of each participating presidency summarising lessons learned, good practices, and recommendations on integrating the technological dimensions of issues on the Council's agenda into the Council's work, including perspectives from civil society; and
- reflect key discussions and lessons on the technological dimensions of issues on the Council's agenda in end-of-presidency wrap-up sessions.

Recommendation 3: Make Better Use of Informal Formats available to Council members

Council members have at their disposal a range of informal meeting formats that may be particularly well suited to addressing the peace and security implications of technology without requiring the inscription of a new agenda item. More systematic and strategic use of these formats could strengthen the Council's ability to engage discreetly and flexibly on the peace and security implications of technological developments.

Meetings held under "Any other business"

The agenda of informal consultations includes "Other matters", also known as "Any other business" (AOB), as a standing item. This may provide a useful format for raising cyber-related incidents or disputes, as discussion under AOB does not generally require consensus to place an issue before members. It therefore allows Council members to raise matters that are not formally on the agenda. In practice, this could offer a closed setting with no public record and limited Secretariat presence in which members could discuss specific cyber incidents. AOB has previously been used to keep the Council informed of developments in situations such as Burkina Faso, Guinea, and Nepal.[337] The AOB convened by Estonia, the UK, and the US in March 2020 to discuss the October 2019 cyberattack affecting multiple institutions in Georgia provides a useful example of how Council members have used this informal format to raise issues relevant to international peace and security arising from cyber incidents.

Informal Interactive Dialogue

In situations involving significant cyber incidents between two or more states, Council members could consider convening an informal interactive dialogue (IID) with officials from the states concerned. This format allows members to hear directly from parties to a conflict or from other interested and affected states in a closed, informal setting.[338] Compared with formal closed meetings, known as "private meetings", IIDs are generally regarded as less politically sensitive and may therefore be better suited to discreet exchanges on situations not on the Council's agenda, where formal consideration could itself carry political implications. In the event of a major cyber incident, an IID could provide a confidential forum for high-level representatives of the parties concerned to exchange views with Council members, including with a view to de-escalation.

The IID format has also been used to facilitate engagement with regional and subregional organisations. In its presidential statement of 13 January 2010, the Council expressed its intention to hold IIDs with such organisations, a practice that has since included regular meetings with senior officials from the AU, the League of Arab States, and the EU.[339] In the context of ICT security, Council members could consider convening IIDs with representatives of relevant regional cybersecurity mechanisms, such as regional computer security incident response teams, to discuss coordination in response to specific incidents or broader regional threat patterns. Such engagement would reflect the growing role of regional organisations in cybersecurity policy and operational coordination and could help connect those efforts to the Council's broader consideration of international peace and security.

[337] Security Council Report. "In Hindsight: Making Effective Use of "Any Other Business"". Monthly Forecast. (April 2016).

[338] IIDs are informal, closed meetings presided over by the Council president and attended by all Council members, and considered proceedings of the Council, while remaining informal and closed. They are not announced in the UN Journal, do not appear in the programme of work, and are reflected only selectively in Council reporting.

[339] Statement by the President of the Security Council (13 January 2010) (S/PRST/2010/1).

IIDs could also be convened to consider the peace and security implications of specific technologies. The July 2019 IID organised by Peru on the challenges and opportunities associated with the use of unmanned aerial vehicles (UAVs) illustrates how Council members have used this informal format to examine specific technologies and their relevance to the Council's work.

Arria-formula meetings

Arria-formula meetings provide another flexible avenue for Council engagement on the peace and security implications of technology and have, in practice, been the format most frequently used for such discussions. Of the meetings convened to date on cybersecurity, most have taken place as open Arria-formula meetings, while a smaller number have been held in the closed format. Experience suggests that the closed format can be particularly valuable where discussions require operational detail, sensitive technical information, or candid exchanges with private-sector actors. A closed Arria-formula meeting convened in October 2021 by Kenya, together with the UN Office on Genocide Prevention and the Responsibility to Protect, for example, brought together major social media companies—including Facebook, TikTok, and Twitter—to discuss the role of online platforms in hate speech and incitement.[340] The format appears to have enabled more candid discussion of internal policies and challenges than would likely have been possible in a public setting. Arria-formula meetings may also gain in credibility and substantive depth when convened jointly with relevant international organisations or UN entities. In the technology domain, Council members could, for example, partner with UNODA or UNIDIR to convene discussions on specific issues.

Open Arria-formula meetings may continue to serve a useful function in raising awareness among Council members and the wider UN membership of specific risks arising from technological developments. Recent examples include discussions on commercial spyware in January 2025.[341]. Where sufficient interest exists, such issues have also been addressed in formal Council meetings, as illustrated by the November 2024 briefing on ransomware attacks on hospitals and other healthcare facilities and services.[342] These examples suggest that technology-related issues can be considered through a range of formats, depending on the sensitivity of the subject matter and the intended audience.

More broadly, while open debates on ICTs, AI, or new and emerging technologies may be appropriate for collective reflection on the evolving threat landscape and the Council's overall role, informal formats are often better suited to focused discussions on specific cyber incidents, regionally situated risks, or the operational implications of technological convergence. More deliberate and consistent use of these tools could help the Council move beyond high-level conceptual engagement towards more practical consideration of how its existing instruments might be applied to the peace and security implications of technology, without prejudging outcomes in parallel UN processes or expanding the Council's formal agenda.

Recommendation 4: Convene Formal Meetings on Specific Cyber Incidents

While informal meeting formats offer flexibility and discretion, particularly for sensitive or technical exchanges, formal Security Council meetings can serve a distinct function in addressing cyber-related incidents in a way that reinforces complementarity with General Assembly-led processes. In particular, they allow members to use the Council's visibility and political authority to draw attention to the framework for responsible state behaviour in the use of ICTs developed through those processes. When used judiciously, such meetings can support the Council's preventive and de-escalatory functions without prejudging responsibility. By invoking agreed commitments and tools in specific situations, Council members can underscore their practical relevance and encourage their use.

A relevant precedent is the meeting held in September 2024 following the submission of a letter by Lebanon to the Council alleging that Israel had carried out a "large-scale cyberattack" involving the detonation of thousands of pagers in the country. In response, Algeria requested a formal briefing under the agenda item "The situation in the Middle East, including the Palestinian question", with a focus on developments in Lebanon. While convened under a longstanding regional agenda item, the meeting nevertheless provided a structured and visible forum for Council members to address the cyber dimension of the situation and its potential implications for regional stability.

During that meeting, Russia stressed that the international community was "not powerless" in the face of the misuse of ICTs, recalling that the global Points of Contact Directory for ICT security had been established through the OEWG process to help prevent and address serious incidents in the information environment and reduce tensions in crisis situations.[343] It called on the parties concerned, first and foremost Lebanon, to make use of the directory, and urged states receiving requests from Lebanon to examine them promptly and respond. The meeting thus showed how formal Council discussions can be used to draw attention to, and encourage use of, tools developed by consensus through General Assembly-led processes, including tools intended to prevent escalation and help manage cyber-related disputes.

Options for Non-Council members and the Broader UN Membership

Recommendation 5: Request the Secretary-General for Recommendations on Security Council-General Assembly Complementarity on ICT Security

The General Assembly considers annually a resolution on the security of and in the use of ICTs. Through such resolutions, member states could request the Secretary-General to provide recommendations on how complementarity between the General Assembly, in particular the Global Mechanism, and the Security Council might be strengthened. Such a request could help clarify how the Council might engage with the peace and security implications of ICT-related developments in a way that builds on, rather than duplicates, the work of General Assembly-led processes.

[340] Security Council Report. "Arria-Formula Meeting on Hate Speech and Social Media". What's in Blue. (27 October 2021).
[341] Security Council Report. "Arria-Formula Meeting on "Commercial Spyware and the Maintenance of International Peace and Security"". What's in Blue. (14 January 2025).
[342] Security Council Report. "Briefing on "Threats Posed by Ransomware Attacks against Hospitals and Other Healthcare Facilities and Services"". What's in Blue. (7 November 2024); Security Council Report. "Arria-Formula Meeting on "Commercial Spyware and the Maintenance of International Peace and Security"". What's in Blue. (14 January 2025).
[343] Security Council Meeting Record (20 September 2024) (S/PV.9730).

There is precedent for this approach in the small arms and light weapons (SALW) agenda. In presidential statement S/PRST/2001/21, the Council requested the Secretary-General for recommendations on how it could address SALW in the situations on its agenda.[344] In his September 2002 report, the Secretary-General recommended closer interaction between the Council and the General Assembly, including in the context of the Programme of Action (PoA).[345] He noted that some member states supported raising the profile of SALW on the Council's agenda, while recognising the need to preserve the distinction between the mandates of the two organs. He further observed that "existing procedures regarding the sharing of information between the Council and the Assembly should be refined, so as to enable both organs to adopt coordinated strategies aimed at promoting a more effective implementation of the PoA by all key stakeholders".

In October 2002, the Council requested the Secretary-General to report on the implementation of those recommendations.[346] In his February 2005 report, he observed that, although "no structured interaction" had yet been established, implementation of the PoA had become "a key issue on the agenda of both organs", and recommended the creation of a small committee to examine how the Security Council and the General Assembly could work together on the issue".[347] While this particular proposal was not implemented, the SALW experience illustrates that the Secretary-General can play a useful role in identifying practical ways to improve complementarity between the Council and the General Assembly in areas where both bodies have relevant, but distinct, responsibilities.

In the SALW case, the initial request came from the Security Council. There appears, however, to be no obvious reason in principle why member states could not seek similar recommendations through a General Assembly resolution, particularly in an area where the Assembly already hosts the intergovernmental process. In the context of ICT security, such a request could invite the Secretary-General to identify practical avenues for cooperation and information-sharing between the Security Council and the Global Mechanism, including on incident-related de-escalation tools, relevant confidence-building measures, and ways in which General Assembly-developed frameworks might inform the Council's consideration of country situations and thematic issues. This would not require reopening debates over institutional mandates. Rather, it could provide a practical basis for thinking through how the two organs might work in a more complementary manner as ICT-related risks increasingly intersect with international peace and security.

Recommendation 6: Revitalise and Repurpose the Group of Friends on E-Governance and Cyber Security to Support Security Council–General Assembly Complementarity

Non-Council members can play a constructive role in strengthening complementarity between the work of the Security Council and the Global Mechanism by revitalising and repurposing the existing Group of Friends on E-Governance and Cyber Security. Established in 2017 to raise awareness, share best practices, and promote capacity-building, the Group of Friends was originally intended to keep the wider UN membership informed of the work of the Group of Governmental Experts at a time when participation in UN cyber discussions was more limited.[348] With the subsequent establishment of the Open-ended Working Group, which was open to all member states, part of that original rationale fell away, and the group's activity appears to have declined accordingly. It could, however, be adapted to serve a more strategic function in the current institutional landscape.

Other Groups of Friends offer useful lessons in this regard. The Group of Friends on Climate and Security, which is open to all member states, has served as a platform for regular briefings on the work of the Security Council's Informal Expert Group on Climate, Peace and Security, helping to socialise emerging analysis and strengthen links between the Council's work and broader UN system efforts.[349] Similarly, the Swiss-led Group of Friends on the Protection of Civilians, established in 2007, has helped maintain momentum on protection issues outside the Council, including through joint statements and support for initiatives led by elected Council members. Over time, it has also broadened its geographical composition, demonstrating how an initially like-minded coalition can gradually evolve into a more representative grouping.[350]

A revitalised Group of Friends on E-Governance and Cyber Security could serve as an informal bridge between the Global Mechanism and the Security Council, facilitating information-sharing and promoting greater alignment between the two forums. In practice, it could help strengthen complementarity by:

- convening regular briefings by the chair of the Global Mechanism and the chairs or facilitators of its thematic groups, as well as by Council members actively advancing these issues in the Council, including, potentially, the chair or co-chairs of a prospective informal expert group on technology, peace and security;
- providing a dedicated space for regular dialogue among the wider UN membership on how the Council and the Global Mechanism can address cyber issues in a complementary manner;
- helping to socialise and build support for any shared political commitments undertaken by Council members, including those associated with a voluntary commitments initiative of the kind described in Recommendation 2;
- supporting the preparation of joint statements delivered at press stakeouts ahead of relevant Security Council meetings and contributing to concept notes for Arria-formula meetings or open debates;
- serving as a forum to share lessons from incident-specific Security Council discussions, including on the use of confidence-building, communication, and de-escalation mechanisms;
- supporting follow-up to practical steps identified in Security Council discussions, including by encouraging use of existing confidence-building tools and facilitating communication on relevant follow-up to the Council; and

[344] Statement by the President of the Security Council (31 August 2001) (S/PRST/2001/21).
[345] Report of the Secretary-General on Small Arms (20 September 2002) (S/2002/1053).
[346] Statement by the President of the Security Council (31 October 2002) (S/PRST/2002/30).
[347] Report of the Secretary-General on Small Arms (7 February 2005) (S/2005/69).
[348] General Assembly Meeting Record (19 September 2017) (A/72/PV.6).
[349] Security Council Report. "The UN Security Council and Climate Change". 2021, No.2. (June 2021); see also Climate Security Mechanism. "Climate Security Mechanism at the United Nations and Group of Friends on Climate and Security announce New Pledges and Partnerships at COP29". (15 November 2024).
[350] Switzerland's seat in the UN Security Council, 2023–2024. "The Protection of Civilians is at the Centre of Attention This Week at The UN in New York" (22 May 2023).

- facilitating continuity between outgoing and incoming elected Council members on cyber-related priorities, including through informal exchanges that support institutional memory and a more coordinated handover of priorities.

In addition to revitalising the Group of Friends on E-Governance and Cyber Security, member states may wish to consider establishing a separate Group of Friends focused on the peace and security implications of AI and other new and emerging technologies. Although two Groups of Friends have already been established on AI, namely the Group of Friends on Artificial Intelligence for Sustainable Development and the Group of Friends for International Cooperation on AI Capacity-Building, neither was created to address the peace and security implications of AI, let alone those of other emerging technologies. Alongside functions similar to those proposed above, such a group could help sustain discussion on where, and in what format, the peace and security implications of AI and other new and emerging technologies might most appropriately be considered within the UN system.

Recommendation 7: Convene Workshops on the Technological Dimensions of Thematic Items on the Council's Agenda

Individual member states interested in mainstreaming the peace and security implications of technology into the Council's thematic work could play a constructive role by convening dedicated workshops on how these issues intersect with established Council priorities, including counter-terrorism, protection of civilians, sanctions, peacekeeping, and WPS. Such workshops could provide a focused setting in which to explore these linkages, exchange lessons learned, and identify where technological considerations may be relevant to ongoing thematic discussions and policy development.

A useful example is the workshop convened by the German Federal Foreign Office in Berlin on 20 and 21 April 2017, entitled "Children and Armed Conflict and Women and Peace and Security: Leading to Change, Closing the Implementation Gap".[351] During its 2011–2012 term on the Council, Germany had chaired the Council's Working Group on Children and Armed Conflict (CAAC). The workshop demonstrates how a member state can advance Security Council priorities by convening a multistakeholder forum. Participants included Security Council members, members of the Groups of Friends on CAAC and WPS, representatives of the UN Secretariat, field practitioners, non-governmental organisations, academics, and policy experts from regional organisations, including the AU, the EU, NATO, and the OSCE. In a later Council meeting, Germany described the workshop as a useful platform for exchanging lessons learned and good practices.[352]

A similar approach could be applied to ICTs, AI, and other new and emerging technologies. Workshops convened by interested member states could examine, for example, how developments in robotics, additive manufacturing, and AI may affect counter-terrorism efforts, sanctions implementation, the protection of civilians, or the operational environment of UN peace operations. They could also help identify where technological developments are already reshaping established thematic agendas, but have not yet been addressed in a systematic way.

Workshops of this kind could offer several benefits. They could create space for the more detailed and practical discussion that is often difficult to sustain in broader thematic meetings, strengthen coherence between technology-related discussions and established Council priorities, and improve awareness and technical understanding among Council members and other stakeholders. Properly designed, they could also generate practical ideas for how existing Council tools and thematic agendas might be applied more effectively to emerging technological challenges.

Options for the UN Secretariat

Recommendation 8: Request Meetings under "Any Other Business" in response to Significant Cyber Incidents or Other Technological Threats affecting UN Operations

Within existing practice, the Secretary-General could request to brief the Council under "Other matters" or "Any other business" (AOB) in order to draw attention to significant cyber incidents or other technological threats affecting UN missions and personnel. The Council's working methods provide that both members and the Secretariat should continue to use the "Other matters" agenda item during informal consultations to raise issues of concern, and they also envisage ad hoc Secretariat briefings in informal consultations when an emergent situation warrants one.[353] Using AOB briefings to raise cyber and other technologically driven risks affecting UN operations would therefore be consistent with existing practice. Such requests would also be in keeping with the spirit of Article 99 of the Charter, under which the Secretary-General may bring to the attention of the Security Council any matter that, in his or her opinion, may threaten the maintenance of international peace and security.

This option could be used in situations involving cyber incidents or other technology-related threats with actual or potential implications for international peace and security. Examples might include malicious cyber activity with significant humanitarian or protection implications in peace operations contexts, cyber operations targeting UN peace operations or other field missions, or cyber-enabled threats directed at peacekeepers or mission personnel, including coordinated online incitement or disinformation campaigns. Other scenarios that could be raised under AOB include the possible use of AI-enabled swarms of armed unmanned aerial systems against UN peace operations or civilians in mission settings.[354] An AOB briefing could provide a timely and discreet forum for informing

[351] Report on the Workshop entitled "Children and Armed Conflict and Women and Peace and Security: Leading to Change – Closing the Implementation Gap" (25 January 2018) (A/72/717-S/2018/65).

[352] Security Council Meeting Record (31 October 2017) (S/PV.8082).

[353] Note by the President of the Security Council (13 December 2024) (S/2024/507), paras. 59 and 67. Paragraph 59 provides that "[t]he members of the Security Council and the Secretariat should continue to use the 'Other matters' agenda item during informal consultations to raise issues of concern." Paragraph 67 further states that Council members intend to continue requesting the Secretariat to provide ad hoc briefings, including in informal consultations, when a situation justifies such briefings.

[354] The UN has highlighted the potential of AI to revolutionise robotic drone swarms, noting that contemporary armed conflicts have shown the increasing use of drones on the battlefield to carry out offensive missions, and adding that with the help of AI, drones could form highly autonomous swarms capable of striking multiple targets simultaneously on a large scale, possibly challenging the principles of proportionality and precaution under IHL. See, UN Regional Centre for Western Europe (January 2025). "UN addresses AI and the Dangers of Lethal Autonomous Weapons Systems"; Some member states and international organisations have also emphasised the threats posed by the use of UAS swarms, including its potential to cause mass casualties or serve as weapons of mass destruction. See, for example, the contributions of Slovenia and the Future of Life Institute, respectively, to the Secretary-General's July 2024 Report on Lethal Autonomous Weapons Systems (1 July 2024) (A/79/88).

Council members of developments that may affect its consideration of country situations on the agenda.

A recent example is the AOB briefing on Mali held on 19 October 2023 in the context of the withdrawal of MINUSMA. The meeting was convened by Brazil, then Council President, following a request from the Under-Secretary-General for Peace Operations, Jean-Pierre Lacroix, and the Under-Secretary-General for Operational Support, Atul Khare. Lacroix and Khare then briefed Council members in closed consultations on the operational difficulties surrounding the withdrawal. The episode demonstrates how the Secretariat can use AOB to bring time-sensitive developments affecting UN operations to the Council's attention. Used selectively, AOB briefings could provide a flexible mechanism through which the Secretariat can alert Council members to technology-related threats facing UN missions and personnel and support more informed consideration of emerging threats.

Recommendation 9: Develop an Aide Memoire on Technology for the Security Council

A practical step for the Secretariat would be to develop an aide memoire on technology for Security Council members. Modelled on the Protection of Civilians (PoC) aide memoire, it could serve as a practical reference tool to support the Council's consideration of the peace and security implications of technology across its existing agenda items and areas of work.[355] It would not create new obligations, but rather consolidate and organise existing Council language and practice in a clear and accessible format.

Building on this report's preliminary aide memoire (see Annex II), the tool could function as a repository of agreed language from Council products, organised by thematic issue and, where relevant, by country situation. By bringing together the ways in which the Council has already addressed technology across different agenda items, it could help systematise an area of practice that remains unevenly documented. Its value would lie in promoting greater consistency, continuity, and analytical clarity over time.

Such a reference tool could also improve both the quality and efficiency of Council engagement. It could assist diplomats in preparing for briefings, consultations, negotiations, and mandate renewals by providing a baseline of existing Council language and practice on the risks and opportunities associated with technology. This could include agreed language on cyber-related threats, such as the use of ICTs for terrorist purposes and the manipulation of information environments. It could also include language on the role of strategic communications in the implementation of UN peacekeeping operations,[356] the need to make better use of available technological tools to enhance situational awareness in peacekeeping missions,[357] and broader commitments to take scientific advances into account more systematically. In addition, the aide memoire could map relevant UN entities, roles, and reporting lines, and identify where existing mandates already intersect with the peace and security implications of technological developments, including in relation to protection tasks, sanctions implementation, and counter-terrorism.

By providing a compendium of potential language for use in negotiations, the aide memoire could support more informed and coherent engagement, improve continuity across successive Council memberships, and facilitate more systematic follow-up across discussions. It could also help sustain informal working methods over time. The experience of the PoC aide memoire suggests that Secretariat-collated information can play an important role in consolidating knowledge and supporting evolving practice, including through informal expert-level engagement. In a similar way, an aide memoire on technology could provide a shared analytical foundation for the possible development of an informal expert group, without requiring a Council mandate, while anchoring deliberations in a clear record of what the Council has previously been able to say, where workable formulations already exist, and where analytical or reporting gaps remain.

Options for Non-Governmental Organisations and the Private Sector

Recommendation 10: Establish a Multi-Stakeholder Working Group on Technology, Peace and Security

Interested stakeholders could establish a multi-stakeholder working group on technology, peace and security, bringing together civil society and non-governmental organisations, private-sector actors, and technical and academic experts with expertise in ICTs, AI, and other new and emerging technologies. Such a group could serve as an external platform for coordination, analysis, and information-sharing aimed at supporting more informed Security Council engagement on the peace and security implications of technological change.

The Counter-Terrorism Committee Executive Directorate (CTED) has engaged technology companies and civil society organisations on the use of the Internet and ICTs for terrorist purposes, including through its joint project with the ICT4Peace Foundation on private-sector engagement and through expert meetings on technology-related challenges.[358] Outside the UN, the Global Internet Forum to Counter Terrorism, launched in 2017 by major technology companies and now operating as an independent non-profit, offers a further example of a structured platform through which technology firms work with governments, civil society, practitioners, and academia on shared security concerns.[359]

These precedents suggest that a more structured interface between the UN and technology-focused stakeholders is both feasible and potentially useful in areas shaped by fast-moving technological risk. This may be particularly important in relation to AI and other emerging technologies, where the pace of innovation can outstrip the UN system's in-house capacity to assess developments in real time. Partnerships with member states, private-sector actors, and academic institutions can therefore help inform consideration of how such technologies might be integrated into operations in a responsible manner.

A comparable working group on technology could help organise

[355] The PoC aide memoire was first compiled by OCHA at the Security Council's request in 2002 and is described by OCHA as a reference tool compiling agreed Security Council language on the protection of civilians, organised by themes. See OCHA. Protection of Civilians Aide Memoire; and Security Council Report. "Protection of Civilians". Monthly Forecast. (May 2024); Another example is the Small Arms and Light Weapons aide memoire. See UNODA (2025). Options for Reflecting Weapons and Ammunition Management in Decisions of the Security Council, Aide Memoire, 3rd ed.

[356] Statement by the President of the Security Council (12 July 2022) (S/PRST/2022/5).

[357] Statement by the President of the Security Council (18 August 2021) (S/PRST/2021/17).

[358] Camino Kavanagh (2017). The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century, Geneva, Switzerland: UNIDIR.

[359] Global Internet Forum to Counter Terrorism Home webpage.

expertise that is currently dispersed across civil society, industry, and research communities. It could facilitate informal information-sharing among stakeholders, identify experts who could serve as briefers in Arria-formula and other informal meetings, and give Council members a clearer sense of the external expertise available on cyber threats and the peace and security implications of technological developments. Similar to the NGO Working Group on WPS, it could also support the development of practical recommendations, and, over time, assist interested members in drafting language for a possible future thematic product on ICTs or AI.

There is already evidence that Council members are interested in drawing on private-sector expertise in this area. As previously mentioned, in October 2021, Kenya and the UN Office on Genocide Prevention and the Responsibility to Protect convened an Arria-formula meeting on hate speech and social media that included representatives of Facebook, TikTok, and Twitter, together with Access Now.[360] More recently, a representative of Google's Threat Analysis Group briefed at the January 2025 Arria-formula meeting on the implications of the proliferation and misuse of commercial spyware for the maintenance of international peace and security,[361] while a representative of Meta's Fundamental AI Research team briefed Council members during the December 2024 meeting on artificial intelligence.[362] These examples underscore the practical value of specialist and private-sector expertise to Council discussions on cyber threats and the peace and security implications of technological developments.

[360] Security Council Report. "Arria-Formula Meeting on Hate Speech and Social Media". What's in Blue. (27 october 2021).

[361] Security Council Report. "Arria-formula Meeting on "Commercial Spyware and the Maintenance of International Peace and Security"". What's in Blue. (14 January 2025).

[362] Security Council Report. "Artificial Intelligence: High-level Briefing". What's in Blue. (18 December 2024).

Annex I: Security Council Thematic Meetings on Technology (2016-2025)

DATE	TITLE	FORMAT	AGENDA ITEM	MEETING RECORD	ORGANISER(S)
24-26 Sept. 2025	Artificial intelligence and international peace and security	Open debate	Maintenance of International Peace and Security	S/PV.10005 and S/PV.10005 (Resumptions I and II)	The Republic of Korea (ROK)
4 Apr. 2025	Harnessing safe, inclusive, trustworthy AI for the maintenance of international peace and security	Arria-formula Meeting			Greece, together with France, and ROK, and co-sponsored by Armenia, Italy, and the Netherlands
14 Jan. 2025	Commercial Spyware and the Maintenance of International Peace and Security	Arria-formula meeting			The US, and co-sponsored by Australia, Austria, Canada, Estonia, Finland, France, Japan, Latvia, Lithuania, the Netherlands, Norway, Poland, ROK, Sweden, and the UK
19 Dec. 2024	Artificial Intelligence and the Maintenance of International Peace and Security	Briefing	Maintenance of International Peace and Security	S/PV.9821	The US
8 Nov. 2024	Threats Posed by Ransomware Attacks Against Hospitals and Other Healthcare Facilities and Services	Briefing	Threats to International Peace and Security	S/PV.9779	The US, with support from France, Japan, Malta, ROK, Slovenia, and the UK
21 Oct. 2024	Anticipating the impact of scientific developments on international peace and security	Briefing	Maintenance of International Peace and Security	S/PV.9753	Switzerland
20 June 2024	Maintenance of international peace and security: addressing evolving threats in cyberspace	Open debate	Maintenance of International Peace and Security	S/PV.9662	ROK
17 May 2024	Unlocking the Potential of Science for Peace and Security	Arria-formula meeting			Switzerland
4 Apr. 2024	Evolving Cyber Threat Landscape and Its Implications for the Maintenance of International Peace and Security	Arria-formula meeting			ROK, together with Japan and the US
19 Dec. 2023	Artificial intelligence: its impact on hate speech, disinformation and misinformation	Arria-formula meeting			Albania and the United Arab Emirates (UAE)
18 July 2023	Artificial intelligence: opportunities and risks for international peace and security	Briefing	Maintenance of International Peace and Security	S/PV.9381	The UK
25 May 2023	The responsibility and responsiveness of States to cyberattacks on critical infrastructure	Arria-formula meeting			Albania and the US, and co-sponsored by Ecuador and Estonia
23 May 2022	Technology and security	Briefing	Maintenance of International Peace and Security	S/PV.9039	The US

Annex I

DATE	TITLE	FORMAT	AGENDA ITEM	MEETING RECORD	ORGANISER(S)
20 Dec. 2021	Preventing Civilian Impact of Malicious Cyber Activities	Closed Arria-formula meeting			Estonia and the UK
28 Oct. 2021	Addressing and Countering Hate Speech and Preventing Incitement to Discrimination, Hostility, and Violence on Social Media	Closed Arria-formula meeting			Kenya and the UN Office on Genocide Prevention and the Responsibility to Protect
18 Aug. 2021	Protecting the protectors: technology and peacekeeping	Open debate	"United Nations peacekeeping operations"	S/PV.8838	India
29 June 2021	Maintaining international peace and security in cyberspace	Open debate	Maintenance of International Peace and Security	S/2021/621	Estonia
17 May 2021	The Impact of Emerging Technologies on International Peace and Security	Arria-formula meeting			China, together with Kenya and Mexico, and co-sponsorship from Egypt, South Africa, and the UAE
2 Oct. 2020	Access to education in conflict and post conflict contexts: Role of digital technology and connectivity	Arria-formula meeting			Belgium, China, the Dominican Republic, Estonia, France, Germany, Niger, Saint Vincent and the Grenadines, and South Africa
26 Aug. 2020	Cyber-Attacks Against Critical Infrastructure	Arria-formula meeting			Indonesia, in cooperation with Belgium, Estonia and Viet Nam, and the ICRC
22 May 2020	Cyber stability, conflict prevention and capacity-building	Arria-formula meeting			Estonia in cooperation with Belgium, the Dominican Republic, Indonesia and Kenya
8 July 2019	The challenges and opportunities of the use of unmanned aerial vehicles (UAVs)	Informal interactive dialogue			Peru
28 Nov. 2016	Cybersecurity and international peace and security	Arria-formula meeting			Spain and Senegal

Annex II: Preliminary Aide Memoire on Technology

COUNCIL PRODUCT	COUNTRY/THEMATIC	CATEGORY	PP/OP
S/RES/1373 (2001)	Counter-terrorism	Terrorist exploitation of communications technologies	"Find ways of intensifying and accelerating the exchange of operational information, especially regarding actions or movements of terrorist persons or networks; forged or falsified travel documents; traffic in arms, explosives or sensitive materials; use of communications technologies by terrorist groups; and the threat posed by the possession of weapons of mass destruction by terrorist groups…"
S/RES/2129 (2013)	Counter-terrorism	Terrorist exploitation of ICTs	"Notes the evolving nexus between terrorism and information and communications technologies, in particular the Internet, and the use of such technologies to commit terrorist acts, and to facilitate such acts through their use to incite, recruit, fund, or plan terrorist acts, and directs CTED to continue to address this issue, in consultation with Member States, international, regional and subregional organizations, the private sector and civil society and to advise the CTC on further approaches…"
S/RES/2250 (2015)	Youth, Peace and Security (YPS)/Counter-terrorism	Terrorist exploitation of ICTs and communications technologies	"Expressing concern over the increased use, in a globalized society, by terrorists and their supporters of new information and communication technologies, in particular the Internet, for the purposes of recruitment and incitement of youth to commit terrorist acts, as well as for the financing, planning and preparation of their activities, and underlining the need for Member States to act cooperatively to prevent terrorists from exploiting technology, communications and resources to incite support for terrorist acts, while respecting human rights and fundamental freedoms and in compliance with other obligations under international law…"
S/RES/2354 (2017)	Counter-terrorism	Terrorist exploitation of ICTs	"Noting with concern that terrorist craft distorted narratives that are based on the misinterpretation and misrepresentation of religion to justify violence, which are utilized to recruit supporters and Foreign Terrorist Fighters (FTFs), mobilize resources, and garner support from sympathizers, in particular by exploiting information and communications technologies, including through the Internet and social media…"
S/RES/2178 (2014)	Counter-terrorism	Terrorist exploitation of ICTs and communications technologies	"Expressing concern over the increased use by terrorists and their supporters of communications technology for the purpose of radicalizing to terrorism, recruiting and inciting others to commit terrorist acts, including through the internet, and financing and facilitating the travel and subsequent activities of foreign terrorist fighters, and underlining the need for Member States to act cooperatively to prevent terrorists from exploiting technology, communications and resources to incite support for terrorist acts, while respecting human rights and fundamental freedoms and in compliance with other obligations under international law…"
S/RES/2396 (2017)	Counter-terrorism	Private-sector cooperation on digital evidence in counter-terrorism	"Encourages enhancing Member State cooperation with the private sector, in accordance with applicable law, especially with information communication technology companies, in gathering digital data and evidence in cases related to terrorism and foreign terrorist fighters…"
S/RES/2341 (2017)	Counter-terrorism	Cybersecurity in counter-terrorism protection efforts	"Recognizing that protection efforts entail multiple streams of efforts, such as planning; public information and warning; operational coordination; intelligence and information sharing; interdiction and disruption; screening, search and detection; access control and identity verification; cybersecurity; physical protective measures; risk management for protection programmes and activities; and supply chain integrity and security…"

Annex II

COUNCIL PRODUCT	COUNTRY/THEMATIC	CATEGORY	PP/OP
S/RES/2617 (2021)	Counter-terrorism	Emerging technologies in counter-terrorism	"Recognizes CTED's work on countering use of the internet, other information and communications technology (ICTs), and other emerging technologies for terrorist purposes, while respecting human rights and fundamental freedoms, and taking into account Member State compliance with applicable obligations under international law, and taking note of the need to preserve global connectivity and the free and secure flow of information facilitating economic development, communication, participation and access to information, and stresses the importance of cooperation with civil society and the private sector in this endeavor..."
		Terrorist use of unmanned aerial systems (UAS)	"Noting with concern the increasing global misuse of unmanned aerial systems (UAS) by terrorists to conduct attacks against, and incursions into, restricted commercial and government infrastructure and public places, acknowledging the need to balance fostering innovation and preventing misuse of UAS as its applications expand, noting international efforts that contribute to raising awareness of and preparedness for terrorist use of UAS as the technology becomes more accessible and broadly used across public and private sectors including the CTED-UNOCT-INTERPOL publication The protection of critical infrastructures against terrorist attacks: Compendium of good practices, the Global Counterterrorism Forum (GCTF) and its Berlin Memorandum on Good Practices for Countering Terrorist Use of UAS..."
S/RES/2663 (2022)	Non-Proliferation (1540 Committee)	Science, technology, and the risk of acquisition of WMD by non-state actors	"Remaining gravely concerned by the threat of terrorism and the risk that non-State actors may acquire, develop, traffic in or use nuclear, chemical, and biological weapons and their means of delivery, and related materials, including by using the rapid advances in science, technology and international commerce to that end..."
S/RES/2686 (2023)	Peacebuilding	Online misinformation and disinformation	"Expressing deep concern at instances of violence fuelled by hate speech, misinformation and disinformation, including through social media platforms..."
S/RES/2729 (2024)	Protection of Civilians/South Sudan	Online misinformation and disinformation	"...further calls upon all parties to refrain from all forms of destabilizing activities, incitement to hatred and violence, and misinformation and disinformation campaigns aimed at UNMISS, including through social media..."
S/RES/2779 (2025)	Protection of Civilians/South Sudan	Online false and falsified information	"...calls upon parties to refrain from spreading false and falsified information undermining UNMISS, including through social media..."
S/RES/2734 (2024)	Counter-terrorism (Sanctions): 1267/1988 Analytical Support and Sanctions Monitoring Team	Use of new and emerging technologies for terrorist purposes	"Expressing concern at the risks posed by the use, in a globalized society, by terrorists and their supporters of information and communications technologies, in particular the Internet, and other new and emerging technologies to facilitate terrorist acts, as well as their use to incite, recruit, fund, or plan terrorist acts..."

Annex II

COUNCIL PRODUCT	COUNTRY/THEMATIC	CATEGORY	PP/OP
S/2022/431 (*draft resolution)	Non-Proliferation/DPRK (1718 DPRK Sanctions Committee)	Malicious cyber activity and ICT-enabled sanctions evasion	"Expresses deep concern over the DPRK's pattern of malicious activity using ICT against other Member States and individuals and entities subject to their jurisdiction, including financial institutions, for the purpose of evading sanctions and contributing to its nuclear and ballistic missile programs, and calls upon all Member States to take appropriate measures within their own jurisdictions, and in accordance with their respective legal processes, to prevent the DPRK and its nationals from using their territories to conduct or facilitate such malicious ICT activity, and clarifies that such measures could include but are not limited to, repatriating to the DPRK any DPRK national conducting malicious activities using ICT-enabled devices or networks and closing businesses associated with any such DPRK nationals from using their territories to conduct or facilitate such malicious ICT activity, and clarifies that such measures could include but are not limited to, repatriating to the DPRK any DPRK national conducting malicious activities using ICT-enabled devices or networks and closing businesses associated with any such DPRK national;"
S/RES/2098 (2013)	UN Peacekeeping/ Democratic Republic of the Congo	Use of technology in arms embargo monitoring	"Monitor the implementation of the arms embargo as described in paragraph 1 of resolution 2078 (2012) in cooperation with the Group of Experts established by resolution 1533 (2004), and in particular observe and report on flows of military personnel, arms or related materiel across the eastern border of the DRC, including by using, as specified in the letter of the Council from 22 January 2013 (S/2013/44), surveillance capabilities provided by unmanned aerial systems, seize, collect and dispose of arms or related materials whose presence in the DRC violates the measures imposed by paragraph 1 of resolution 2078 (2012), and share relevant information with the Group of Experts..."
S/PRST/2021/17	UN Peacekeeping	Technology in UN peacekeeping	"The Security Council recognizes that technology has the potential to act as a force multiplier by enhancing performance, saving resources, simplifying work processes, and allowing peacekeeping missions to have a deeper understanding of the environments they operate in, through improved collection, analysis and dissemination of data; further emphasizing that existing and new technologies can support the safety and security of peacekeepers and the protection of civilians, by enabling effective and timely decision-making including through early warning and response...." "The Security Council encourages better integration of existing and new technologies, especially digital technology, to enhance field support, implementation of safety and security, and protection of civilians tasks of Security Council mandates, and encourages troop- and police contributing countries and field missions to support field-focused, reliable, and cost-effective technologies that are driven by the practical needs of end users on the ground, including taking into consideration a gender perspective, consistent with international human rights law and international humanitarian law, and in this regard stresses the need for consultations with Member States and host countries, as appropriate...." "The Security Council encourages the Secretary-General to provide updates on the use of new technology in supporting United Nations peacekeeping missions, as appropriate, in his periodic reporting."
S/PRST/2024/6	Technology	Systematic consideration of scientific advances	"The Security Council expresses its continued commitment to take into account scientific advances more systematically, where appropriate, and in line with its mandate, in as far as their impact on international peace and security is concerned."

Security Council Report Staff

Shamala Kandiah Thompson
Executive Director

Katerina Limenopoulou
Chief Operating Officer

Paul Romita
Managing Editor

Alina Entelis
Deputy Managing Editor

Dawit Yirga Woldegerima
Deputy Managing Editor

Vladimir Sesar
Development and Outreach Manager

Audrey Waysse
Operations Manager

Andrew Azzopardi
Policy Analyst

Sara Bertotti
Policy Analyst

Matthew Blainey
Policy Analyst

Erik Ramberg
Policy Analyst

Gaurav Redhal
Policy Analyst

Rodrigo Saad (Lead author)
Policy Analyst

Ashley Onwuzuruike
Research Intern

Security Council Report is a non-profit organisation supported by the Governments of Australia, Austria, Bahrain, Carnegie Foundation, Cyprus, Denmark, Finland, Friedrich-Ebert-Stiftung, Germany, Ireland, Konrad-Adenauer-Stiftung, Kuwait, Latvia, Liechtenstein, Luxembourg, Malta, the Netherlands, Norway, Open Society Foundations, Portugal, Republic of Korea, Singapore, Spain, Switzerland, Türkiye, United Arab Emirates, and Individual Contributions.

Design Point Five, NY

Security Council Report
125 Park Avenue
New York NY 10017

Telephone +1 212 759 9429
Web securitycouncilreport.org

Security Council Report would like to thank the government of Singapore for its generous support of this project. We also express our gratitude to all colleagues who generously shared their perspectives on the topics and issues covered in this report.