GENEVA GRADUATE INSTITUTE

GLOBAL GOVERNANCE CENTRE

Science and Technology at the United Nations Security Council (Part 2):

Cybersecurity and New Technologies

Hayley Umayam, Geneva Gradudate Institute

Aurel Niederberger, Geneva Gradudate Institute

GENEVA GRADUATE INSTITUTE

INSTITUT DE HAUTES ÉTUDES INTERNATIONALES ET DU DÉVELOPPEMENT

GRADUATE INSTITUTE OF INTERNATIONAL AND DEVELOPMENT STUDIES

Acknowledgements:

We wish to thank the participants of the workshop "**Leveraging Diplomacy with Science at the UN Security Council: Lessons and Avenues for Cyber & Emerging Technologies**", held in Geneva on April 28, 2022. Thanks go to Amb. Alexandre Fasel and the panellists, Roxana Radu, Megan Roberts, Francesca Bosco, Megan Roberts, and Nicolas Seidler. We are particularly grateful to our interviewees for sharing their knowledge with us. This includes Alisha Anand, Neil Davison, Myriam Dunn Cavelty, Samuele Dominioni, Amandeep Gill, Katharina Höne, Martin Mandveer, Roxana Radu, Erik Reichborn, Megan Roberts, and Paul Romita. Further interviewees from the United Nations are not named here but likewise deserve our gratitude. The project benefited from crucial support by Jonas Pasquier, Esther Neuhaus, Samir Yeddes, Gaël Restrepo Barman, Achim Wennmann, Monique Beerli, Sylvia Nissim, and Annabelle Littoz-Monnet. Special thanks are in order for Roxana Radu for her extended feedback and for so generously sharing her time and knowledge. Finally, we thank the Swiss Federal Department of Foreign Affairs (FDFA) for indispensable support.

Despite the support received, this report reflects exclusively the views of the authors. Neither does it express the views of the FDFA nor of any of the persons mentioned above.

This report was authored by Hayley Umayam and Aurel Niederberger. It is part of a two-part written output of the project "Leveraging Diplomacy with Science at the UN Security Council" that was co-supervised by Aurel Niederberger, Thomas Biersteker, and Grégoire Mallard. The principal study was conducted in 2022; tables are up to date until April 2024.

May 2024

Table of Contents

Table of Tables

List of Abbreviations

AOB	“Any Other Business” (Security Council)
AFM	Arria-Formula Meeting
AI	Artificial Intelligence
AWS	Autonomous Weapons Systems
CCS	Climate Change and Security
GGE	Group of Governmental Experts
ICRC	International Committee of the Red Cross
ICT	Information and Communication Technology
IO	International Organisation
ML	Machine Learning
NGO	Non-Governmental Organisation
OEWG	Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security
P5	The Permanent Five (Security Council members)
SCR	*Security Council Report* website
UK	United Kingdom
UN	United Nations
UNGA	United Nations General Assembly
UNSC	United Nations Security Council
US	United States of America
WPS	Women, Peace and Security

Executive Summary

The United Nations (UN) Security Council (UNSC) is tasked with ensuring international peace and security, an important mandate made even more challenging due to a range of new and emerging threats. While science, expertise, and evidence can inform decision-making at the Security Council, there are significant challenges to reaching consensus around many topics. This report provides insight into the challenges and opportunities involved in utilising science and expertise at the Security Council with a focus on information and communication technologies (ICT), thus complementing report 1 in this series, *Science and Technology at the United Nations Security Council (Part 1): Leveraging Diplomacy with Science*.[1] In particular, this report analyses the use of formal and informal sources and topic framing in Security Council deliberations and events on cybersecurity and emerging technologies to assess how they facilitate or hinder consensus.

Most formal discussions on issues related to ICT and security in the UN have taken place at the level of the UN General Assembly (UNGA). However, a few years ago, the Security Council began grappling with the linkages between ICT and international peace and security. Many are calling on the Council to dedicate more attention to the impact of cybersecurity and emerging technologies on the issues on its agenda, as well as to consider cybersecurity and emerging technologies as their own issue areas. Despite these calls—and the increasingly common discussion of these topics at the Council—those seeking to promote ICT as a formal agenda item must navigate not only a complex geopolitical environment but a range of complicating factors particular to cyber and emerging technology. The fields of cybersecurity and emerging technologies encompass vast, rapidly evolving issue areas. Much of their content requires specialised expertise to both understand and act upon, exacerbating unequal access to information about cyberspace. Furthermore, while some efforts to establish norms of good behaviour in cyberspace exist, a lack of conceptual and operational clarity about the various elements remains.

In this context, science and expertise are crucial when navigating these evolving challenges. However, as argued in the complementary report in this series, science and expertise can also be deeply linked to politically sensitive issues or can themselves be politicised or have a political agenda. The resources, expertise, and technical know-how associated with the ICT track make it particularly prone to geopolitical sensitivities. Nonetheless, both reports find that science and technical expertise can help open up spaces of discussion, particularly by offering helpful ways of framing or narrowing down a topic to locate areas of agreement. In the ICT track, such topic framing can highlight existing points of consensus and carefully build on them.

Report Outline and Key Findings

Using document analysis and expert interviews, this report surveys the status of the ICT track at the Security Council. The methodology and analytical approach underpinning these findings are described in *Part 1: Leveraging Diplomacy with Science*. **Section 1** of this report maps out the status of cyber and emerging technologies at the Security Council, using case studies

[1] Niederberger, Aurel and Hayley Umayam. 2022. *Science and Technology at the United Nations Security Council (Part 1): Leveraging Diplomacy with Science.* Geneva: Global Governance Centre.

to assess potential entry points and stumbling blocks. While only enjoying their first dedicated formal meeting in 2016, a recent increase in formal and informal Security Council events on ICT issues indicates growing acceptance of their relevance. Nonetheless, there have only been a few formal meetings and decisions related to these topics, providing a limited source of precedents upon which to advance the track. While some ICT-related discussions were broadly framed and characterized by direct confrontation between participants, others focused on specific applications with selective reference to UN documentation, particularly those that highlight important collaboration.

Section 2 looks more closely at the specific use of science and expertise as a way of understanding the best entry points for science-enhanced diplomacy in the ICT track. The predominance of informal settings, such as Arria-formula meetings (AFMs), as a venue for discussion has allowed for a wide range of actors to be invited as experts, especially from the private sector. These informal meetings are sometimes broadly framed, allowing for multiple perspectives and issue areas to be considered; however, this puts debates at a risk of being both vague and confrontational. Other meetings were more narrowly framed around an established area of the Council's mandate, such as peacekeeping. However, we also see that **a member state's choice of framing and use of expertise need not be aimed at a formal outcome; some states view ICT as an area where signalling their adherence to objectivity and evidence is itself an important outcome**.

Section 3 provides a matrix of possible topics to be pursued in the ICT track. Informed by interviews with experts on cybersecurity and emerging technologies, the matrix maps topics in the field of ICT onto established Security Council agenda items. The matrix also indicates the sensitivities of different topics at the Council at the time of analysis (July 2022), providing rough sketches of known political considerations and expected controversies surrounding each topic. The purpose of this matrix is to provide quick access to topics that can be pursued in the ICT track. The topics can be further tailored in line with the framework proposed in *Part 1: Leveraging Diplomacy with Science*.

The report **concludes** by synthesising the three sections and reflecting on what framing and sources have been directly and indirectly useful for promoting consensus in the ICT track.

Section 1: The ICT Track at the UNSC

Since 2016, a range of Security Council meetings have been dedicated to issues that can be grouped under a broader ICT track. It is important to recognise that while observers of the UNSC (such as the think tank Security Council Report) categorise ICT as a thematic track at the Council, no formal agenda item on cybersecurity or emerging technologies at the Security Council yet exists. In comparison to the UNGA, which has given attention to matters of cybersecurity and emerging technologies for over two decades, the Security Council has only recently begun considering this topic.[2] Nonetheless, the Council has already touched upon

[2] The General Assembly had already dedicated a resolution to "developments in the field of information and telecommunications in the context of international security" in 1999 (A/RES/53/70). Furthermore, the UNGA mandated six subsequent *Groups of Governmental Experts (GGEs)* on cybersecurity since 2004. Over time, these groups worked out a corpus of recommendations (or "norms") on the regulation of cyberspace and on government action. Among the major agreements reached by the GGEs is that international law is applicable to cyberspace. In 2018, efforts at the General Assembly were split into two tracks. A resolution sponsored by the USA (A/RES/73/266) mandated the sixth GGE. In the same year, a resolution sponsored by Russia (A/RES/73/27) created the *Open-Ended Working Group on Developments in the Field of Information and Telecommunications in*

several topics under this theme. By the middle of 2022, the ICT track saw at least 11 Council meetings—12, if counting the discussion under "Any Other Business" (AOB) and the 2020 joint statement). However, only two of those were formal debates. The most recurring topic has been cybersecurity, which has been addressed with either a broad perspective or a focus on critical infrastructure protection against cyberattacks. Beyond that, a range of other topics have been the primary or secondary focus of meetings. Symptomatic of the difficult standing that many ICT-related issues have at the Security Council, these topics have mostly been discussed in AFMs (i.e., informally).

The first meeting fully dedicated to ICT and international peace and security was a November 2016 AFM on cybersecurity hosted by Spain and Senegal. The concept note circulated ahead of this AFM attempted to broaden the discussion of ICTs and international security by including the potential role of ICTs in exacerbating existing tensions and the importance of protecting ICT-dependent critical infrastructure.[3] Previously, discussions of ICT at the Council primarily focused on their potential exploitation in terrorist activities, a risk formally recognised in UNSC resolution 2129 (2013).[4]

Table 1 gives an overview of formal and informal meetings at the Council under the ICT track to date, primarily utilising the categorisation of events presented by the *Security Council Report (SCR)*.[5] The following list cites meetings in which ICT themes of cybersecurity or emerging technologies were the explicit topic or subtopic of discussion; we do not list every event where ICT themes may have been mentioned.

Table 1: Key Events (ICT Track)[6]

Topic	Subtopics[7]	Event Type	Sponsors	Year
Cybersecurity	Challenges resulting from use of ICT that may threaten international peace and security.	AFM	Spain, Senegal	Nov 2016

the Context of International Security (OEWG), which was chaired by Swiss ambassador Jürg Lauber. Several countries—including the European Union—brought an initiative underway to reconcile efforts by the General Assembly under a third initiative (the *Programme of Action*), which would replace the other two fora.

[3] Security Council Report. 2016. "Open Arria-formula Meeting on Cybersecurity." https://www.securitycouncilreport.org/whatsinblue/2016/11/open-arria-formula-meeting-on-cybersecurity.php.

[4] *Ibid.* Similarly, shortly before the November 2016 AFM on cybersecurity, Ukraine hosted an AFM on counterterrorism that considered terrorist attacks on critical infrastructure, including through cyber means (the vulnerability of critical infrastructure to cyberattacks would become a recurrent item on the Security Council's agenda).

[5] The November 2016 AFM (on protection of critical infrastructure against terrorist attacks) initiated by Ukraine is not included on the SCR's list, presumably because it was presented under the counterterrorism theme. Similarly, the August 2019 Debate (on peace and security in the Middle East) initiated by Poland is not included in this list, as cybersecurity was mentioned in remarks but was not formally part of the topic. This event is nonetheless referenced in subsequent Open Debates on ICT (the June 2021 Open Debate initiated by Estonia). Likewise, a May 2021 AFM ("Delivering Accountability through Innovation and Partnership: Harnessing Technology to Deliver Justice") initiated by Iraq, the Netherlands, the United Kingdom (UK) and the United States (US) has not been included in the SCR list, presumably because it relates to subsidiary bodies.

[6] The analysis contained in this report reflects key events in the ICT track up to May 2022. Table 1 contains events up to April 2024 .

[7] Where the original concept notes were not available, Security Council Report briefs serve as source for sub-topics.

Topic	Subtopics[7]	Event Type	Sponsors	Year
Hybrid Wars	Changed nature of warfare due to increasing use of new technologies and strategies (includes cyber technologies and propaganda).	AFM	Ukraine	Mar 2017
Cyber Threats and Hybrid Warfare	Malicious use of cyber.	Informal meeting ("AOB") Joint statement issued	Estonia, United Kingdom (UK), United States (US)	Mar 2020
Cyber Stability, Conflict Prevention and Capacity Building	"Existing norms, policies and cooperation mechanisms for advancing cyber stability, conflict prevention and capacity building on global, regional and national level."[8]	AFM	Estonia, in cooperation with Belgium, Dominican Republic, Indonesia, and Kenya	May 2020
Cyberattacks Against Critical Infrastructure		AFM	Indonesia, in cooperation with Belgium, Estonia, and Viet Nam, and the International Committee of the Red Cross	Aug 2020
Education in Conflict	"Access to education in conflict and post conflict contexts: Role of digital technology and connectivity."[9]	AFM	Belgium, China, the Dominican Republic, Estonia, France, Germany, Niger, Saint Vincent and the Grenadines, and South Africa	Oct 2020
Impact of Emerging Technologies on International Peace and Security	Artificial Intelligence (AI), digital technology, biotechnology, and material technology.	AFM	China, in cooperation with Kenya and Mexico, and with non-UNSC members Egypt, South Africa, United Arab Emirates	May 2021
Maintaining International Peace and Security in Cyberspace		Open Debate (**First formal meeting**)	Estonia	Jun 2021

[8] Security Council Report: *What's in Blue. Arria-formula Meeting: Cyber Stability, Conflict Prevention and Capacity Building.* 21 May 2020. Online at: https://www.securitycouncilreport.org/whatsinblue/2020/05/arria-formula-meeting-cyber-stability-conflict-prevention-and-capacity-building.php.

[9] Security Council Report: *What's in Blue. Arria-formula Meeting: Access to education in conflict and post-conflict settings.* 1 October 2020. Online at: https://www.securitycouncilreport.org/whatsinblue/2020/10/arria-formula-meeting-access-to-education-in-conflict-and-post-conflict-settings.php.

Topic	Subtopics[7]	Event Type	Sponsors	Year
Protecting the Protectors: Technology and Peacekeeping	Emerging technologies and peacekeeping; protection of civilians.	Open Debate (Presidential Statement)	India	Aug 2021
Hate Speech and Social Media		AFM (closed)	Kenya	Oct 2021
Preventing Civilian Impact of Malicious Cyber Activities	Preventing cyberattacks on critical civilian infrastructure	AFM (closed)	Estonia, UK	Dec 2021
Digital Technologies & Maintaining International Peace and Security		Briefing	US	May 2022
The Responsibility and Responsiveness of States to Cyberattacks on Critical Infrastructure	Ensuring a secure and peaceful cyberspace; responsibility of states to intervene with cyber threats emanating from their territory; public-private partnerships.	AFM	Albania, US, with co-sponsorship by Ecuador and Estonia	May 2023
Artificial Intelligence: Opportunities and Risks for International Peace and Security	Promoting safe and responsible development of AI; AI for peace and security; Emerging risks caused by AI in terms of exacerbating conflicts.	Briefing	UK	Jul 2023
Artificial Intelligence: Its Impact on Hate Speech, Disinformation and Misinformation	AI and hate speech/ misinformation, election interference; AI for cyberattacks; Public-private partnerships	AFM	Albania, United Arab Emirates	Dec 2023
Evolving Cyber Threat Landscape and its Implications for the Maintenance of International Peace and Security	Ransomware, cryptocurrency theft, and malware; the impact of cyber-crime on WMD non-proliferation.	AFM	Republic of Korea, co-hosted by Japan and the US	Apr 2024

As shown in **Table 1**, discussion of ICT topics tends to be initiated by non-permanent Security Council members, with fewer than half of ICT events being initiated or co-sponsored by one of the five permanent members (P5). After Spain and Senegal's ground-breaking AFM in 2016, Estonia became a principal promoter of cybersecurity questions at the Security Council. Estonia announced cybersecurity as a priority for its Security Council membership 2020-2021, subsequently organising various events. For example, Estonia organised an AFM on "Cyber Stability, Conflict Prevention and Capacity Building" in May 2020. It also co-organised a

December 2021 closed AFM on "Preventing Civilian Impact of Malicious Cyber Activities" with the UK and co-sponsored two further AFMs in 2020 (one on cyberattacks against critical infrastructure with Indonesia in August and one on access to education in conflict and post-conflict contexts with Belgium in October). More significantly, Estonia organised an Open Debate in June 2021, which was the first formal meeting on cybersecurity ever held at the Security Council. While this Open Debate did not lead to a formal outcome, it nonetheless set a precedent for future discussions by directly tabling cybersecurity as a matter of international peace and security.[10] Meanwhile, the diversity of sponsors and co-sponsors (involving E10 and P5, from all continents and including China, although not Russia) demonstrates a growing consensus around the fact that cyber and emerging technologies fall under the UNSC's mandate.

ICT Track Challenges

Despite the increasing frequency of discussions, progress in the ICT track remains difficult to achieve. There has been only one formal outcome with an explicit ICT focus.[11] Part of the difficulty is that the ICT track (and cyber in particular) is subject to the same risks of politicisation outlined in *Part 1: Leveraging Diplomacy with Science*. For instance, many topics (such as cyberattacks) carry implicit questions of attribution, which can be politically sensitive given past confrontations between member states in the cyber realm.[12] Therefore, as with women, peace and security (WPS) and climate change and security (CCS), ICT champions must navigate a complex geopolitical environment. This environment includes different states with different visions of the future and of the role of the Council and other actors, as well as different levels of expertise necessary to discuss cyber challenges, leading to a range of different interests and incentives.[13]

In the ICT track, broader debates such as sovereignty and multilateralism often underpin discussions of the applicability of international law to cyberspace and the appropriate venue for addressing emerging concerns. Therefore, even if the most recent ICT discussions at the UNSC indicate a general consensus regarding the topic's relevance to international peace and security (see: **Case Study B: Digital Technologies**), particular elements within the track remain contentious. Although many states agree with the premise that humanitarian law should apply to cyberspace, some may wish for this discussion to be consigned to the OEWG. Similarly, some states may advocate for other venues besides the UNSC to discuss questions of how emerging technologies affect terrorist recruitment and funding.[14]

---

[10] Interview #4.

[11] There was a Presidential Statement (S/PRST/2021/17) following India's 2021 Open Debate. Security Council Report. 2021. "Peacekeeping: Open Debate, Resolution and Presidential Statement." https://www.securitycouncilreport.org/whatsinblue/2021/08/technology-and-peacekeeping-open-debate.php.

[12] Interview #4. In rarer cases, such attribution is explicitly made, such as in the joint statement issued by the US, UK, and Estonia in 2020. This was the first time a specific cyberattack was discussed at the Council (https://un.mfa.ee/estonia-in-the-security-Council-the-first-year/).

[13] Interviews #1, 3, and 5.

[14] Interview #9.

In addition to these challenges to science-enhanced diplomacy at the UNSC, which are common across all tracks, the nature of ICT poses additional unique barriers. First, the fields of cyber and emerging technologies are new and rapidly evolving, encompassing a vast number of issue areas and a range of techniques without clear conceptual or operational definitions. Much of this confusion is due to the ambiguous possibilities inherent in emerging technologies (i.e., any given technology's potential benefits and risks). While our findings show greater opportunity for technical experts to weigh in on ICT matters, the inordinate number of topics that could be considered ICT—or that fall within the categories of cyber or emerging technologies—makes it unrealistic to expect that decisionmakers could have a nuanced and up-to-date understanding of all issues.[15]

This broad topical range is made even more problematic without common understandings of terms, concepts, and activities. While states may reference the potential risks and misuse of cyber and emerging technologies, there are no agreed thresholds or norms outlining the potential impacts or harm caused.[16] Even defining particular types of activity, such as cyberterrorism, remain contested at the international level.[17] Promoting common definitions is a crucial step in building consensus about appropriate behaviour in cyberspace.[18]

Second, much of the content of ICT discussions requires advanced or technical knowledge that can be incomprehensible for non-specialists. Explanations of cyber events or the misuse of emerging technology—especially if the effects are not immediately tangible—can be difficult to simplify. This means that policymakers and public stakeholders are to a larger extent dependent on technical expertise to recognise and evaluate a potential problem or threat.[19] While our findings show increased opportunities for technical experts to weigh in on ICT matters, formal Security Council meetings remain the domain of member state representatives who must prioritise how they receive and leverage information on a wide range of global issues.

Third, there is unequal access to data and information about cyberspace, with obvious implications for the ability to identify actors behind a cyberattack. Intelligence services, and governments with high cyber capabilities, and some private companies, enjoy levels of access to information that are not available to the UNSC as a whole or to other stakeholders, such as academics, non-governmental organisations (NGOs), and the public.[20]

ICT Track Confrontations

Much more than any WPS and CCS issues, the core themes of the ICT track have been raised in the context of direct confrontations between member states. Two particularly confrontational episodes in the ICT track point to the tensions that are likely to keep overshadowing future events, particularly if they involve cybersecurity. The first one was Ukraine's 2017 AFM on hybrid wars (a type of warfare that includes cyberattacks and online disinformation campaigns). Ukrainian ambassador Volodymyr Yelchenki stated in his opening remarks that

[15] Interview #5.
[16] Interview #6.
[17] Interview #1.
[18] Interview #9.
[19] Interviews #3 and 4.
[20] Interview #6. This problem is also found in other policy domains at the Security Council, such as counterterrorism.

"[t]he most commonly cited recent example of hybrid warfare is the Russian aggression against Ukraine."[21]

In a second episode in 2020, the Georgian Permanent Representative (not a Security Council member state) wrote a letter to the Security Council, raising allegations of a coordinated cyberattack against the Georgian Government and media websites (S/2020/135). Estonia, the UK, and the US raised the issue as AOB on 5 March 2020. In a subsequent joint press statement, these three countries expressed that they "are clear that Russia's military intelligence service–the GRU–conducted these cyberattacks in an attempt to sow discord and disrupt the lives of ordinary Georgian people."[22] The statement continued:

> *"These cyber-attacks are part of Russia's long-running campaign of hostile and destabilizing activity against Georgia and are part of a wider pattern of malign activity. These actions clearly contradict Russia's attempts to claim it is a responsible actor in cyberspace and demonstrate a continuing pattern of reckless GRU cyberoperations against a number of countries."*[23]

Despite the obstacles facing the ICT track at the Security Council, two events respectively hosted by China and India also show that the track is deemed important across some of the usual political blocks in the Council (see case studies below). That said, convergence between these states and Western states remains minimal, and the UNSC's responsibility over this set of issues is outspokenly contested by Russia.

Case Study A: Emerging Technologies at the UNSC—China's AFM on Emerging Technologies vs. India's Open Debate on the Technological Capabilities of Peacekeeping Missions[24]

Until 2021, the ICT track focused on matters of cybersecurity and cyberattacks on critical infrastructure. (Other) emerging technologies only moved into the spotlight with an AFM on "the impact of emerging technologies on international peace and security" held in 2021 and, shortly thereafter, with an Open Debate on "technology and peacekeeping" that led to the first ICT-related Presidential Statement. While one event focused on **technological capabilities**, the other event focused on specific **needs to be covered by technology**. Comparing the two events demonstrates how discussions around some of the same technologies can either turn

---

[21] Website of the government of Ukraine. 2017. "Opening Remarks by Ambassador Volodymyr Yelchenko at the AFM of the UNSC on Hybrid Wars." https://ukraineun.org/en/press-center/181-opening-remarks-by-ambassador-volodymyr-yelchenko-at-the-arria-formula-meeting-of-the-unsc-on-hybrid-wars/ (accessed on December 23, 2021).

[22] Joint Statement by Estonia, the United Kingdom, and the United States at a Press Availability on Russian Cyberattacks in Georgia, as reprinted on the website of the U.S. Mission to the United Nations New York, March 5, 2020. URL: https://usun.usmission.gov/joint-statement-by-estonia-the-united-kingdom-and-the-united-states-at-a-press-availability-on-russian-cyberattacks-in-georgia/ (accessed on December 21, 2021).

[23] *Ibid*.

[24] Analysis based on the video recordings of the two meetings. China's AFM was organised with Council members Kenya and Mexico, with cooperation from other non-Council member states. It was held virtually on 17 May 2021. United Nations. 2021. "UN Security Council Arria-Formula Meeting on 'the Impact of Emerging Technologies on International Peace and Security'." https://media.un.org/en/asset/k10/k10mt4ffo6. India's Open Debate on Peacekeeping was held on 18 August 2021 as a signature event during its Council presidency. United Nations. 2021. "United Nations peacekeeping operations: Technology and peacekeeping – Security Council, 8837th meeting." https://media.un.org/en/asset/k15/k15ee8t8qg.

into heated exchanges and verbal attacks or garner enough consensus to lead to new Security Council outcomes.

In the AFM on "the impact of emerging technologies on international peace and security" (May 2021), the Chinese representative that co-hosted the meeting focused on the potential for economic development driven by emerging technologies, and the need to grant developing countries fair access to emerging technologies. The Chinese representative furthermore emphasised the potential benefits of emerging technologies to peacekeeping, counterterrorism, and non-proliferation, stressing that "great improvements are needed to improve the equipment and capabilities of peacekeeping operations to ensure the safety and the security of peacekeepers."

It is noteworthy that interviewees held an optimistic view on the set-up of this AFM.[25] On their own, China's concept note and opening remarks, which promoted the potential benefits of emerging technologies, provided a hopeful framing that invited collaboration. Our assessment of the actual dynamics and statements of the meeting is less positive, however. After the concept note and the opening remarks highlighted the benefits of emerging technologies, other speakers did not shy away from confrontation.

The Kenyan representative pointed at similar potential benefits as the Chinese representative but also warned of the risks that emanate from the great powers. Alluding to both cyber conflict and disinformation campaigns, he pointed at:

> *"the threat that I think comes to the world … when great powers have rivalry over the future of the internet. … It is crucial that the UN provides more multilateral frameworks to mitigate the impact of such cyber rivalries and create a broad middle ground that allows countries such as ours to enjoy a free and open internet: political speech that is accurate, we are able to have free speech that is as free of fake news as possible without it rising into forms of censorship on the internet."*

The UK speaker began by pointing to "so much potential good" of emerging technologies:

> *"[UNITAD] generate evidence to bring justice to survivors of Daesh atrocities … In Syria to provide early warning to civilians of impending airstrikes, and in Yemen, the Office of the UN special envoy has made technology integral to the monitoring plans for the proposed national ceasefire."*

However, the UK speaker followed up these hopeful remarks with direct critique of negative uses of technology by Myanmar, which also served as implicit critique of other UNSC member states:

> *"But, as we've heard from so many other speakers, we share the concerns when we see authoritarian states using technology to control and censor. We see surveillance technology used to monitor and persecute citizens, denying them their human rights. And we saw this recently when the military junta shut down the internet in Myanmar, denying a free press or free speech. And we see states*

[25] Interview #5.

deliberately trying to disrupt and destabilize other states by undermining their political systems with hostile state actors and criminal gangs deliberately targeting democratic processes, including elections."

The misuse of technologies by some member states was also a theme in the US representative's remarks:

"We need to be cognisant of the fact that emerging technologies can also be used to do harm. For example, under the guise of protecting public order, security or countering terrorism, some are using facial recognition software and genetic sequencing technologies to assert political and social control, limit online and offline spaces, and target journalists, human rights defenders, and members of civil society through censorship and unlawful or arbitrary surveillance. (…) Certain emerging technologies, if exploited by outside malicious actors, can further damage democracy and human rights, and the functioning of transparent, market driven economies. Here in the United States, foreign actors have misused technology to interfere in our democratic elections, attack our critical infra-structure, and steal our intellectual property."

In sum, this broadly conceived AFM touched on many issues without leading to concrete results. It revealed the lack of a shared definition of emerging technologies and entailed multiple confrontations.[26] Overall, the AFM steered in a direction that was likely not what China had anticipated or wanted, judging from its opening statement. Many representatives struck a more critical and even aggressive tone, with China itself unambiguously being a target of this critique.

Later that year (Aug 2021), India organised an Open Debate on "technology and peacekeeping" that unfolded very differently. In contrast to the AFM, this debate was confined to a specific application of technology, namely in peacekeeping missions. Consensus emerged naturally under this topic framing, as states shared the general opinion that "the right technology helps keep peacekeepers safe and it helps them keep the communities they serve safe, too."[27] Some countries, such as the US, still stressed the need to ensure that peacekeeping missions use innovative technologies responsibly and that surveillance, reconnaissance, and unmanned aircraft systems must be "used in line with UN doctrine and policy." However, there were no direct attacks or diversions into other applications of emerging technologies in this debate. In the end, India could claim one of the signature events of its Presidency to have yielded in the first Presidential Statement on technology and peacekeeping.

As this case study shows, technologies can simultaneously serve purposes that are unanimously supported by the Security Council and other purposes that are controversial. A debate focused on such technologies at large can therefore quickly move from agreeable issues to open dispute. Careful tailoring of the topic may prevent such open dispute, although potentially at the cost of circumventing the most pressing issues. The Open Debate chaired

[26] UK representative: "From the breadth of discussion today, it's clear that we have no shared definition of emerging technologies. … We must remain focused on where the Security Council can add value to these debates."

[27] Remarks by the US Ambassador Linda Thomas-Greenfield at the Open Debate on Protecting the Protectors: Technology and Peacekeeping, on August 18 2021 (S/PV.8838).

by India suggests that a debate **focused on specific technological needs rather than general technological capabilities can be more coherent and less contentious**.

Case Study B: Digital Technologies at the UNSC—US-sponsored Briefing on Digital Technologies and Maintaining International Peace and Security (May 2022).[28]

While no formal outcome was sought, the points of agreement and disagreement made at the May 2022 Briefing on "Digital Technologies and Maintaining International Peace and Security" provide a useful stock-take of the ICT track. Similar to the broadly framed AFM in 2021, the 2022 Briefing, initiated by the United States, considered both the potential benefits and risks of technology. Already established in the August 2021 Open Debate and Presidential Statement, the potential *benefits* of technology applied to the specific matter of peacekeeping were cited by many in the May 2022 Briefing, providing the participants with a basic common understanding in a conversation otherwise still characterised by diverging views.[29] Examples cited relating to the potential *risks* of technology were more overtly political, given the context of the Russian invasion of Ukraine.

None of the statements at this most recent Council discussion indicated that ICT should *not* be considered a matter of international peace and security. Rather than challenging the appropriateness of the Council as a venue to discuss ICT, multiple states asserted that the Council has a role to play on such matters, in addition to the work of other UN bodies. Invited briefers, such as the Under-Secretary-General for Political and Peacebuilding Affairs, cited recent reports of the Secretary General (A/74/821) to emphasise the link between digital technologies and human rights, and therefore support the topic's relevance, including to the Council.

There was less clarity on what would constitute the use of technology for "good" more generally, and which actors should abide by which set of standards or rules. Multiple voices called for the development of a normative framework or code of conduct to establish standards of responsible behaviour, citing efforts at the level of the General Assembly (OEWG, and the Secretary-General's call for a Global Digital Compact). However, questions also lingered on the role of private companies and NGOs vis-a-vis international peace and security.

Overall, there appears to be consensus that the benefits and risks of ICT are matters of concern for the Council, at least with ICT framed as broadly as it was at this event.[30] The 2022 Briefing still provided a stage for several open confrontations, like the equally broadly framed 2021 AFM did. However, repeated references to the 2021 presidential statement provided the discussion with an anchor point that was missing in the earlier AFM, even though this

[28] Analysis based on meetings coverage of SC/14899 (United Nations. 2022. "Political Affairs Chief Spells Out Double-edged Nature of Digital Technologies, in Briefing to Security Council." https://www.un.org/press/en/2022/sc14899.doc.htm) and available remarks by one of the briefers (United Nations DPPA. 2022. "Remarks by Under-Secretary-General Rosemary DiCarlo to the Security Council on Technology and Conflict." https://dppa.un.org/en/remarks-under-secretary-general-rosemary-dicarlo-to-security-Council-technology-and-conflict).

[29] This consensus around using technology to improve the safety, security and efficiencies of peacekeeping is also described in expert interviews (Interview #5).

[30] Interview data also supports this point, that States do not "demonise" technology as a whole but increasingly discuss it in terms of the benefits and risks. Interview #1.

presidential statement captures consensus around a more narrowly framed topic (peacekeeping).

Section 2: Experts and Science

Experts and briefers in the ICT Track

The substantive challenges of the ICT track also create opportunities to leverage diplomacy with science. The vast, rapidly evolving and highly technical nature of ICT necessitates high engagement with expertise. Interviews suggested that a key contribution of expertise in the ICT track is to provide synthesised accounts of developments using simplified and actionable language.[31] Furthermore, despite specific areas of agreement, the ICT track remains contentious, with very few UNSC-documents to draw on in debates. Findings presented in *Part 1: Leveraging Diplomacy with Science* indicate that, in the absence of UNSC-documents, the council gives more weight to other UN-mandated expertise and, if that is scarce, too, to external science.

Interviewees have also suggested that there is growing recognition that expertise in the digital and technology space, even as far as international security is concerned, is not always exclusive to government sources—it is increasingly held by private sector and academic sources.[32] Some member states have already publicly advocated for more cooperation with the private sector, academia, and civil society.[33] Indeed, it may be these sources that put emerging technologies on the radar of policymakers in the first place.[34] **Table 2** shows the types of experts invited to recent ICT events at the Council.

Table 2: Specific Uses of Expertise in the ICT Track

Year	Event Type	Invited Experts (Briefers)
2016	**AFM** Spain, Senegal	**Private Sector** ▪ Telefonica Internacional USA ▪ FireEye iSIGHT Intelligence **Non-UN NGOs or international organisations (IOs)** ▪ ICT4Peace foundation ▪ US Amb. to OSCE and Chair of the Working Group on elaborating cyber confidence-building measures
2017	**AFM** Ukraine	**Academia/think tanks/research institutions** ▪ Norwegian Institute of International Affairs ▪ Rutgers University (US) **State agencies** ▪ Fund for National Strategies (Ukraine)

[31] Interviews #1, 5.

[32] Interview #5.

[33] May 2020 AFM organised by Estonia. Ministry of Foreign Affairs of Japan. 2020. "Security Council Arria-Formula Meeting: Cyber Stability, Conflict Prevention and Capacity Building." https://www.mofa.go.jp/fp/cp/page24e_000253.html.

[34] Interview #1.

2020	**AFM (May)** Estonia	**UN officials** ▪ High Representative for Disarmament Affairs **Academia/think tanks/research institutions** ▪ Technology and Public Policy Program at the Center for Strategic and International Studies (US) **State agencies** ▪ Cyber Security Agency of Singapore
	AFM (Aug) Indonesia	**UN officials** ▪ Under-Secretary-General for Humanitarian Affairs and Deputy Emergency Relief Coordinator at OCHA ▪ United Nations Institute for Disarmament Research **Non-UN NGOs or IOs** ▪ International Committee of the Red Cross
	AFM (Oct) Belgium	**UN officials** ▪ UN Children's Fund ▪ Telecommunication Development Bureau, International Telecommunication Union **State agencies** ▪ National Agency for Information Society of Niger ▪ Ministry of ICT and Innovation of Rwanda
2021	**AFM (May)** China	**UN officials** ▪ Disarmament Affairs ▪ Department of Economic and Social affairs and Office of the Secretary-General's envoy on technology **Academia/think tanks/research institutions** ▪ Stockholm International Peace Research Institute
	Open Debate (Jun) Estonia	**UN officials** ▪ Disarmament Affairs
	Open Debate (Aug) India	**UN officials** ▪ Secretary-General of the UN
	AFM (closed, Oct) Kenya	**UN officials** ▪ Under-Secretary-General and Special Advisor on the Prevention of Genocide and UN Focal Point on Hate Speech **Private Sector** ▪ Facebook ▪ Twitter ▪ TikTok **Non-UN NGOs or IOs** ▪ Access Now
	AFM (closed, Dec)	**UN officials** ▪ Disarmament Affairs

	Estonia	**Non-UN NGOs or IOs** ▪ International Committee of the Red Cross
2022	**Briefing** US	**UN officials** ▪ Under-Secretary-General for Political and Peacebuilding Affairs **Non-UN NGOs or IOs** ▪ Global Voices/Advox **Academia/think tanks/research institutions** ▪ McGill University (Canada)

There have only been two formal debates specifically on ICT topics. The predominance of the AFM as a venue has allowed a wide range of actors to be invited as experts. Besides various UN officials, including the UN High Representative of Disarmament Affairs, invited briefers included the head of a national cyber security agency (Chief Executive of the Cyber Security Agency of Singapore), representatives of two NGOs (ICT4Peace and Access Now), and the president of the International Committee of the Red Cross (ICRC). Also invited were experts from various think tanks and research institutions, including the United Nations Institute for Disarmament Research and the Stockholm International Peace Research Institute. The selection of experts—more than the actual framing of the event topics—demonstrates specific interest at the intersection of cyber questions with disarmament or arms control.

What stands out in the ICT track, however, is the large number of invited experts from the private sector. These included the CEO of *Telefonica Internacional* and the director of a cybersecurity company called FireEye iSIGHT, as well as representatives of social media companies such as Twitter, Facebook, and TikTok. In fact, the ICT track is illustrative of a specific benefit of science-enhanced diplomacy at the UNSC. Given its peculiar nature, the UNSC is strongly restricted in terms of the type of actors it can engage with; unlike other international institutions, it does not engage in multi-stakeholder dialogues or public-private partnerships.[35] When it comes to the governance of cyberspace and AI, however, dialogue with a range of governmental and non-governmental stakeholders (including private technology providers) is generally deemed to be indispensable. At the Security Council, the common solution to achieving some direct inclusion of these stakeholders is to invite them as experts, typically to AFMs.[36]

The inclusion of such different types of actors can also help address the challenge of access to information about the ICT track (such as classified information or private sector-owned data not being available at the Council). Interviews suggest that informal meetings, such as retreats or AFMs, provide opportunities to involve expertise from academia and the private sector, noting that UNSC members have a large appetite to learn about this set of issues.[37] The involvement of experts from a wider range of sectors can also increase the flow of information

[35] Although the Security Council has, over the past two decades, increasingly engaged the private (financial) sector in the context of its sanctions legislations, it has done so indirectly by imposing Chapter-VII based demands on member states, rather than seeking coordinated efforts with the private sector.

[36] Diplo Foundation, for instance, lists the following actors as important stakeholders in the governance of cyberspace: government and regulatory authorities, judicial and law enforcement institutions, private sector and technology communities, and NGOs and academia. Representatives of all these groups have been invited as experts to AFMs. Diplo Foundation: *Science Diplomacy.* Online at: https://www.diplomacy.edu/topics/science-and-diplomacy/ (last accessed: 11.7.2022).

[37] Interview #5.

in the *other* direction, i.e., the dissemination of concerns discussed at the Security Council to practitioners in different domains.

The diversity of briefers (in terms of institutional affiliations) invited to informal meetings provides opportunities to leverage diplomacy with science as it opens the doors to a vast range of expertise to be involved in UNSC events. In other regards, however, briefers have been less diverse. While NGO briefers hail from global or non-Western backgrounds, most briefers from academia and think tanks stem from Western institutions (mostly in Northern America). A similar effect can be noted for briefers from the private sector, which tend to stem from big social media companies based in the US and China. Thus, increasing technical expertise at the UNSC risks further benefitting those countries that are already at an advantage in terms of the research institutions (or companies) that they host.[38]

The "Hierarchy of Sources" in the ICT Track

Part 1 of this series introduced the idea that there is an informal *hierarchy of sources* at play during Security Council debates. While many states substantiate their arguments by referring to scientific/expert sources of information, there is a preference for citing formal UNSC documents on the same topic if they are available. If the Council has not agreed on any decisions related to a given topic, including if states have questioned the appropriateness of a topic to the Council's mandate, there are fewer Council documents available to cite in arguments. In these instances, states that try to bring a new issue onto the Council's agenda preferably resort to science and expertise to establish a causal link between a given phenomenon of concern and international peace and security. If available, member states furthermore show a clear preference for UN-produced expertise over external science.
The types of sources referenced in Security Council debates therefore further indicate the state of a track. Due to the absence of meeting minutes of informal events, it is impossible to thoroughly review all references made during ICT events.[39] Unlike the emerging practice seen in the WPS track where convening states circulate remarks as a letter following an AFM, many of the statements or concept notes made for informal ICT track events remain unavailable to the public. This perhaps speaks to the slow progress of the track as a whole and the continued need for informal spaces of discussion. Nonetheless, a preliminary investigation indicates that in the 13 ICT events held to date, frequent references are made to UN initiatives or processes (especially the GGE, OEWG, and various initiatives of the Secretary-General), the experiences of affected states,[40] and the UN Charter. Interviewees suggest that the attention on the "consensus reports" by the GGE and OEWG—both GA-level bodies concerned with

[38] We only have anecdotal evidence pointing to such an effect. The problem may also be of a practical nature. Sponsors of UNSC events may find it difficult to identify adequate briefers from outside the UN-system. This encourages them to look for briefers in institutions that they are familiar with, which tend to be a limited number of established players, such as the best-known universities and think tanks. These, in turn, are disproportionately located in the Western hemisphere. A practical solution to this challenge may be to identify focal points in the scientific community early on before proposing events at the UNSC. Such focal points (e.g., from research foundations and universities) should have a better overview of the international scientific community or can point to North/South research collaborations where these exist. Alternatively, where (Western) sponsors of a UNSC event do not find expert briefers from other regions of the world, they can go through other Member States. For instance, Belgium's AFM included briefers from relevant government agencies in Rwanda and Niger.

[39] It is possible to make certain inferences based on summaries or previews of events, such as those available at SCR. Occasionally, some states publicise their written remarks but not systematically enough to facilitate thorough review. For an example see Permanent Mission of Estonia to the UN. 2020. "Statement by DPR Gert Auväärt at Arria-formula meeting 'Access to education in conflict & post conflict contexts: Role of Digital Technology & Connectivity'.".https://un.mfa.ee/statement-by-dpr-gert-auvaart-at-arria-formula-meeting-access-to-education-in-conflict-amp-post-conflict-contexts-role-of-digitaltechnology-amp-connectivity/.

[40] See Part 1: Leveraging Diplomacy with Science, p. 44.

international norms and cybersecurity—is a useful way for UNSC members to draw on existing consensus at a global level.[41] It is also likely that invited experts from outside the UN referenced other types of sources (think tank reports and research of civil society organisations, for instance).

There is more documentation available from formal Council events, even if there have been few so far in the ICT track. The first Open Debate on an ICT topic was Estonia's signature event in June 2021 on cybersecurity, followed by India's Open Debate on technology and peacekeeping in August of the same year. Although they yielded different outcomes, both were arguably successful by different metrics. Comparing these two events provides insights not only into the tailoring of themes, but also the types of sources successfully used in the ICT track.

Examining the specific sources referenced during these formal events, we find that the conveners limited their framing and remarks to sources considered to be relatively high in the *hierarchy of sources*. **While multiple AFMs related to ICT and/or to cyberspace occurred before these Open Debates in 2021, neither the concept notes nor convener remarks referenced these informal Council events.[42]** Rather, Estonia's concept note for the June 2021 event referred to other formal Council events, particularly Open Debates. None of the Open Debates cited in the concept note were explicitly on cyber or ICT, but were nonetheless used to assert this topic as part of a broader debate on international security, noting that the debates "have demonstrated that, for many countries, cyberthreats are a matter of concern and constitute a key security challenge."[43] Estonia's concept note and remarks also referenced international law and existing UN initiatives, as well as their own state experiences.[44] Likewise, India's concept note on peacekeeping did not reference any AFMs. India's concept note did not even reference Open Debates where ICT or emerging technologies were mentioned, such as Estonia's Open Debate two months earlier, dissociating their debate from any comparably more contentious debates. Instead, it foregrounded the safety and security of peacekeepers and cited existing strategies at the General Assembly level (such as the Secretary General's Digital Transformation Strategy for UN Peacekeeping). No other Council documentation was explicitly cited in India's concept note, perhaps seen as unnecessary given the foregrounding of UN peacekeeping missions.

Based on the available remarks and summaries of these events, **none of the P5 made references to Council documentation or events,** whether AFMs, previous debates, or other materials. The closest references to Council activities made by the P5 during the Open Debates related to the experiences of peacekeeping missions. Rather, they cited international law, UN agencies and existing UN initiatives, multi-stakeholder initiatives, or state experiences. **By contrast, a few elected member states cited the previous AFMs** (particularly those in 2020), and even made a thematic link with a Council resolution (not focused on ICT). Additionally, many discussed the Council's own activities as being conducted

41

42 However, at the June 2021 Open Debate, the remarks of a few Council members did reference previous AFMs (see below). Meeting records are not available for August 2021 Open Debate.

43 S/2021/540 concept note circulated by Estonia ahead of June 2021 Open Debate on "Maintaining international peace and security in cyberspace."

44 Estonia's remarks cited only positive examples of their country's experiences with cyber, not mentioning specific cyberattacks.

in or connected to cyberspace.[45] Invited experts, exclusively UN officials, chose to reference the experiences of UN peacekeeping missions or UN agencies and initiatives outside of the Council. Together, these findings suggest that **those pushing for an agenda item (conveners) or with the most clout (P5) remain quite selective about the sources they choose to reference at these formal meetings, while elected members choose to capitalise on the variety of venues and formats in which ICT has been discussed as they express support for an agenda item**. Accordingly, **elected members also rely more on those formats and sources where external science and expertise are usually included and heard**.

Table 3: Comparing Sources in ICT Open Debates

Convener	Estonia (June 2021)	India (August 2021)[46]
Sources in concept note and/or remarks by convening state	**UNSC sources** Open Debates (Dec 2017,[47] Aug 2019,[48] Apr 2021[49]) **UN sources** Normative frameworks and international law (UN Charter), existing UN initiatives[50] **Other** Own state experience, regional platforms/initiatives	**UN sources** UN agencies or initiatives,[51] experiences of UN missions
Sources and references made by invited experts/briefers	**UN sources** Secretary-General statements, reports, and initiatives; existing UN initiatives;[52] UN Charter	**UN sources** UN agencies or initiatives [55]experiences of UN missions

[45] Such as virtual reality (VR) visits to Colombia or conducting formal and informal meetings online.

[46] Convening state remarks from: Ministry of External Affairs: Government of India. 2021. "Remarks by External Affairs Minister at the UN Security Council Open Debate on Technology & Peacekeeping." https://mea.gov.in/Speeches-Statements.htm?dtl/34192/Remarks+by+External+Affairs+Minister+at+the+UN+Security+Council+Open+Debate+on+Technology++Peacekeeping; other state remarks from: Permanent Mission of the Republic of Indonesia to the United Nations, New York. 2021. "The Security Council Ministerial Open Debate 'Protecting the Protectors: Technology and Peacekeeping." https://kemlu.go.id/newyork-un/en/news/15689/the-security-Council-ministerial-open-debate-protecting-the-protectors-technology-and-peacekeeping#; United States Mission to the United Nations. 2021. "Remarks by Ambassador Linda Thomas-Greenfield at a UN Security Council Open Debate on Protecting the Protectors: Technology and Peacekeeping." https://usun.usmission.gov/remarks-by-ambassador-linda-thomas-greenfield-at-a-un-security-Council-open-debate-on-protecting-the-protectors-technology-and-peacekeeping/; and Government of Ireland. 2021. "Joint Nordic statement at the Security Council Open Debate on 'Protecting the Protectors: Technology and Peacekeeping'." https://www.government.is/diplomatic-missions/embassy-article/2021/08/18/Joint-Nordic-statement-at-the-Security-Council-Open-Debate-on-Protecting-the-Protectors-Technology-and-Peacekeeping/

[47] On contemporary challenges to international peace and security (S/PV.8144), cybersecurity mentioned.

[48] On challenges to peace and security in the Middle East (S/2019/643), cyberthreats and cyber incidents mentioned.

[49] On the "protection of civilians in armed conflict" (S/2021/415), threats of malicious cyber activities on critical infrastructure mentioned.

[50] GGE reports.

[51] Then forthcoming strategy for the digital transformation of UN peacekeeping; UN Partnership for Technology in Peacekeeping; Action for Peacekeeping; UNITE Aware platform.

[52] GGE reports and OEWG.

[55] Initiatives mentioned include: strategy for the digital transformation of UN peacekeeping; UN Partnership for Technology in Peacekeeping; Roadmap for Digital Cooperation; UNITE Aware platform. United Nations. 2021. "Remarks at Security Council High-Level Open Debate on United Nations Peacekeeping Operations: Technology and Peacekeeping." https://www.un.org/sg/en/content/sg/speeches/2021-08-18/remarks-security-Council-debate-un-peacekeeping-operations-technology-and-peacekeeping.

	Other Regional platforms/initiatives, private sector initiatives,[53] multi-stakeholder initiatives[54]	
Sources and references made by other states during discussion[56]	**UNSC sources** AFMs[57] **UN sources** UN Charter, UN agencies,[58] existing UN initiatives[59] **Other** Other state experiences, regional platforms/initiatives, multi-stakeholder initiatives,[60] own state experience or state leadership	**UNSC sources** Res 2538 (2020);[61] **UN sources** UN agencies or initiatives[62]

By one metric, the India Open Debate was more successful because it yielded a Presidential Statement and resolution on the introduced topic with little pushback.[63] These were the expected outcomes of their signature event. By contrast, it does not appear that Estonia expected to achieve a specific outcome but rather to foster discussions on the topic.[64] In that regard, the strategy and framing employed by Estonia have their merits. Rather than successfully producing a formal outcome, interviewees observed that Estonia's biggest accomplishment was simply putting cybersecurity on the Council's agenda.[65]

Box 1: Topic Tailoring in the ICT track

In addition to selecting sources, there are different strategies for **tailoring topics** in the ICT track. Estonia's concept note presented cybersecurity as a threat to international peace and security and highlighted dangers for civilians. This framing is akin to partially narrowing down the area of scientific/technical concern (Alternative #1) and foregrounding vulnerable groups (Alternative #5),

[53] Microsoft's Cybersecurity Tech Accord; Siemens' Charter of Trust; Kaspersky Lab's Global Transparency Initiative.

[54] Paris Call for Trust and Security in Cyberspace.

[56] Indicative selection of remarks only, limited by sampling and/or by availability.

[57] Bahrain (not specified), Belgium (citing 2020 AFM on cyberattacks on critical infrastructure), Ecuador (citing 2020 AFM "on the subject"), Latvia (citing 2020 AFM on increasing relevance of cybersecurity for international peace and stability).

[58] Office of Counter-Terrorism.

[59] GGE and OEWG; 2030 Agenda for Sustainable Development.

[60] Paris Call for Trust and Security in Cyberspace.

[61] On the participation of female peacekeepers.

[62] Then forthcoming strategy for the digital transformation of UN peacekeeping; Action for Peacekeeping; UNITE Aware platform; Roadmap for Digital Cooperation; UN Digital Toolkit in peace mediation.

[63] The resolution passed (Res 2589 (2021)) cited other UNSC resolutions like resolution 2518 (2020) and resolution 2378 (2017) on the safety and security of peacekeepers and on reporting, respectively. The Presidential Statement (S/PRST/2021/17) references the Secretary-General's Action for Peacekeeping and initiatives like the UNITE Aware platform.

[64] Based on its campaign, Estonia's signature events on cyber were meant to raise awareness of cyber challenges to international peace and security, explore questions regarding the Council's role, and foster discussion on enhancing the implementation of existing norms of responsible state behaviour in cyberspace. However, Estonia did circulate a draft Presidential Statement on cybersecurity to Council members (Security Council Report. 2022. "In Hindsight: The Security Council and Cyber Threats, an Update." https://www.securitycouncilreport.org/monthly-forecast/2022-02/in-hindsight-the-security-Council-and-cyber-threats-an-update.php; and Security Council Report. 2021. "June 2021 Monthly Forecast." https://www.securitycouncilreport.org/monthly-forecast/2021-06/cybersecurity.php).

[65] Interview #9.

as discussed in the previous report (*Part 1: Leveraging Diplomacy with Science, Section 2*).[66] Interviewed experts suggest that **Estonia was able to foster some level of agreement around the otherwise contentious issue of cybersecurity by promoting a civilian perspective**.[67] Instead of discussing specific aspects or examples, Estonia made claims regarding the Council's responsibility to "ensure the protection of civilians and civilian objects in situations of armed conflict," including cyberspace.[68] The rest of Estonia's remarks were broad, mentioning cyberspace and "harmful cyberactivities" without explicitly mentioning cybersecurity. In contrast, India's concept note foregrounded the specific needs of UN peacekeeping missions and potential benefits technology brings to them (Alternative #6). Part of India's success is attributed to its degree of specificity, tailoring the topic of emerging technologies to an agreed-upon Council mandate area (see **Case Study A: Emerging Technologies**).

Section 3: Potential ICT Topics at the UNSC

We designed and conducted a survey of 13 experts in the fields of cybersecurity and emerging technologies in the security domain with the objective of identifying resources and topics that could be effective, based on our insights in the prior sections. The following **Topics Matrix** serves as a tool for quick access to relevant topics and as a basis to explore further topics beyond the ones listed. Likewise, these topics can be further tailored to raise the chance of reaching agreements in the Security Council.[69] The Topics Matrix is structured as follows: the columns are divided into important themes in cyber/new technologies, while the rows are divided into established topics at the Security Council. Some of these topics are less controversial than cyber/new technologies *per se* and can provide a more consensual framework within which to discuss the same ICT issues. This applies in particular to sustainable peace, protection of civilians, effectiveness of the UN, peacekeeping, and terrorism. Accountability, on the other hand, will always make for an explosive topic in combination with cyber-issues at the Security Council. Accountability is nonetheless included in the table due to its particular relevance. Likewise, any discussion of cybersecurity will also be at least somewhat controversial at the Security Council.

Topics that have already been the primary subject of a meeting are marked in blue. For topics that have not been treated or treated only marginally at the Security Council, a three-colour-scale (green/yellow/red) indicates its expected degree of controversy at the Council. Note that these are estimates based on the controversy that topics or certain elements therein have sparked on other occasions or based on the degree to which it has implications for the internal or external actions of a member state. As these conditions can change quickly, the table only

[66] See Part 1 in this series (*Part 1: Leveraging Diplomacy with Science*) which identified the following topic tailoring as alternatives to broad and general topics:

1. Narrowing down the scientific / technical concern by focusing on a more specific sub-issue.
2. Narrowing down the scientific / technical concern by focusing on the regional / conflict-specific security effects of an issue.
3. Focusing on the *exacerbating* effects of an issue on *existing* risks to security that are already acknowledged by the Security Council.
4. "Wrapping" the topic in another thematic or geographic track.
5. Foregrounding vulnerabilities (rather than, e.g., offensive capabilities).
6. Foregrounding specific needs of the UN to fulfil its mandate, e.g., needs of UN missions.

[67] Interview #9.

[68] S/2021/621

[69] See Part 1 in this series: Niederberger, Aurel and Hayley Umayam. 2022. *Leveraging Diplomacy with Science: Science and Technology at the United Nations Security Council.* Geneva: Global Governance Centre.

provides a snapshot. The degree of controversy at the Council further varies depending on the precise topic tailoring and which states might be implicitly criticized.[70] The **Appendix** provides a first orientation on the topics in the rows "protection of civilians," "sustainable peace," and "effectiveness of the UN."

Leveraging Recent Events

In identifying potential ICT topics at the Security Council, it is important to be aware of recent events that may highlight certain challenges, provide opportunities for discussion, or alter a topic's sensitivity at the Security Council. Interviewees highlighted two recent global events as having high salience for the Security Council.

First, the **COVID-19 pandemic sparked a massive wave of disinformation worldwide.** Interviewees suggest that the research related to the "virality" of mis/disinformation, showing the unprecedented speed of its spread, resonates with decisionmakers.[71] Interviewees suggest that the scale and universality of the threat of COVID-19 disinformation prompted significant action and leadership around an emerging problem, with the UN deciding to play an active role in what they perceived as a global problem.[72] Likewise, the international security implications of misinformation have been picked up in a variety of Council events. The topic of social media's negative effects on peace and security was touched upon during Estonia's June 2021 Open Debate and given more specific attention (as "hate speech") during Kenya's closed AFM in October that year. The latter built on the momentum of the former in advocating for the use of social media for both early-warning and pre-emptive measures. Together, these UNSC events along with the wide range of actions to counter misinformation more widely indicate a willingness to discuss this topic at high levels and may present an entry point for discussing ICT themes more generally.

Second, the cyberattack on the ICRC in November 2021 constituted a major breach of humanitarian data. So far, this event does not appear to have been specifically discussed at the Council.[73] It is possible that reluctance to discuss the attack on humanitarian infrastructure is due to political sensitivities around attribution.[74] Interviewees echoed this hesitation, noting that directly highlighting this event as an attack on humanitarian infrastructure would be contentious. Rather, interviewed experts identified this event as a potential rallying point to encourage further discussions about responsible online behaviour for states.[75] With this consensus-seeking framing, the event could be used to reiterate the applicability of international humanitarian law to cyberspace, or to promote the need for civilian protection given the privacy concerns with data breaches.[76]

---

[70] *Ibid.*

[71] Interview #5.

[72] See for instance the UN's "Verified Initiative" and "Pause" campaigns (United Nations. 2021. "UN 'Pause' campaign has helped slow spread of life-threatening misinformation." https://news.un.org/en/story/2021/07/1095222).

[73] Reports indicate that the ICRC attack took place in November 2021. There was an AFM on the prevention of civilian impact on malicious cyber activity organised by Estonia and the UK in December 2021, but the ICRC attack had not yet been detected. Based on publicly available documentation, it also appears that formal and informal meetings on relevant topics that took place after the detection of the attack did not directly mention the event.

[74] While no attribution has been made publicly, ICRC's analysis on the techniques and procedures involved reportedly fits the profile of a state or "state-like" actor.

[75] Interview #9.

[76] Interview #9.

Table 4: Topics Matrix

- Central topic of an earlier AFM or formal meeting at the Security Council.
- Not a central topic of an earlier AFM/formal meeting at the Security Council:
  - Lower political sensitivity to be expected
  - Medium political sensitivity to be expected
  - High political sensitivity to be expected

<table>
<tr><td>Established UNSC Topics/ Topics in ICT</td><td>Cybersecurity</td><td>Artificial intelligence (AI) and Machine Learning (ML)</td><td>Emerging technologies (other than AI)</td><td>Cryptocurrencies / Blockchain & FinTech</td><td>Social Media & Civilian Online Activities</td></tr>
<tr><td rowspan="2">Protection of Civilians (see also peacekeeping)</td><td rowspan="2">Protecting civilians against cyberattacks.</td><td>Discrimination by AI/ML applications.</td><td>Digital tech supporting humanitarian action such as humanitarian corridors (e.g., drone-protected), demining, etc.</td><td rowspan="2">Financial technologies for unbanked crisis zones.</td><td>Internet shutdowns to mask human rights violations.</td></tr>
<tr><td>Protection of civilians against automated weapons systems (AWS).</td><td>Access to education in conflict.</td><td>Access to information in conflict.</td></tr>
<tr><td rowspan="3">Sustainable peace</td><td rowspan="3">Cyber and electoral security.</td><td>Deep fakes and other advanced disinformation and deception tools as risks to sustainable peace.</td><td rowspan="3">Tech for good; tech for climate, etc. (big data, biotech, nanotech).</td><td rowspan="3">Preventing corruption in public spending through e-procurement systems (optionally blockchain-based).</td><td>E-government / ICT for citizen empowerment & inclusion of women and youth in governance, mediation, and peacebuilding; bridging divided communities.</td></tr>
<tr><td></td><td>Hate speech & disinformation in social media.</td></tr>
<tr><td></td><td></td></tr>
</table>

Effectiveness of the UN	Protection of the UN secretariat and UN experts/investigators against cyberattacks.	Integration of AI & ML (e.g., supporting decision-making) in UN missions.	New technologies and effectiveness of the UN.	Biometrics and software applications to register identities in UN refugee camps (optionally blockchain-based) (also Prot. of Civ.).	Transparency of UN activities, citizen engagement, information & participation.
Peacekeeping	Protecting peacekeepers (and other humanitarian actors) against cyberattacks.	Tech for situational awareness (1): satellite image recognition; scanning (social) media for adverse content and to rapidly gain understanding of local perceptions.	Tech for situational awareness (2): mobile communication centres, unmanned aerial vehicles, sensors/security devices, tethered observational balloons, advanced software; tech in the "military grade" category including intel, surveillance, and reconnaissance.	Use of blockchain in peacekeeping operations (e.g., for data protection or for automating and increasing transparency and traceability of aid distribution).	Mis/disinformation threats to peacekeeping ops.
Arms control	Offensive Cyber Capabilities (control measures thereof).	Autonomous Weapons Systems (AWS).	Drones. Digital technologies to monitor compliance with arms control agreements.	Cryptocurrencies and proliferation financing (sanctions evasion, ransomware).	Use of social media to detect arms embargo violations.
Terrorism	Cyberattacks by terrorists (notably on critical infrastructure).	Mass surveillance in counterterrorism.	Drones used for terrorist purposes.	Cryptocurrencies and financing of terrorism (sanctions evasion, ransomware).	Social media and terrorist propaganda / recruitment.
Accountability	Attribution of cyberattacks.	Minimal human control over & responsibility for AWS.	Digitally derived evidence and digital forensics.	Tracing transactions of cryptocurrencies (“follow the money”).	Responsibility of social media companies for content (e.g. hate speech).
Protecting critical infrastructure	Cyberattacks on critical infrastructure.	AI / ML for the protection of critical infrastructure against cyberattacks.	Drone attacks on critical infrastructure.	Ransomware attacks on critical infrastructure.	Internet access during conflict (see Protection of Civilians: access to information in conflict).

Conclusion: Ways Forward for ICT and Science-enhanced Diplomacy at the Security Council

Whether as a risk or an opportunity, matters of ICT are increasingly included in discussions of international peace and security. Cybersecurity and emerging technologies are by their nature political and contentious topics, yet their contemporary salience is inescapable to the Security Council. Paying attention to the use of expertise in discussions of ICT topics at the Security Council provides a variety of lessons for how science-enhanced diplomacy can be leveraged in sensitive issue areas.

Given the potential contentiousness of cybersecurity and emerging technologies, this report has found great importance in the tailoring of discussion topics. Security Council events can be carefully framed to confine the debate on certain technologies for the sake of constructive discussions and outcomes, as seen in India's Open Debate on peacekeeping and technologies. However, events may also be more deliberately framed for the sake of frank debates without the ambition of a formalised outcome, as seen in Estonia's Open Debate on cybersecurity. In both cases, repeated references to consensus around a more narrowly framed topic, such as peacekeeping, or to the desire to seek consensus, such as General Assembly-level processes at the OEWG or GGE, show a commitment to the relevance of ICT.

In fact, the framing of a Security Council discussion and the types of expertise utilised need not only be about achieving a formal outcome or holding a discussion on the Council. The inclusion of multiple sources of expertise and multiple sites of discussion are helpful for providing information to decision makers and disseminating it more widely. The dissemination of scientific arguments can ultimately help increase the number of "access points" or spaces for compromise, helping achieve some of the other benefits of science-enhanced diplomacy such as building norms. For instance, not only did Estonia's Open Debate firmly establish cybersecurity as a matter of concern for the Security Council, but the sources and framing also contributed to public diplomacy, particularly by playing a truth-telling role.

AFMs have become unique spaces to incorporate broader expertise, as shows the common inclusion of non-UN experts.[77] But while AFMs provide opportunities to introduce topics and bring in a variety of expertise, Council members still seem to be proceeding cautiously in formal events, where they rely primarily on established sources and topics, hesitating to refer even to its own informal events. For instance, while six AFMs focused on ICT and/or cyberspace had occurred before the first formal Open Debates on ICT in 2021, neither the concept notes nor convener remarks in the formal debates referenced these earlier informal Council events. In fact, the sources referenced by the conveners of such formal Council events and by P5 members show that they remain quite selective, mainly drawing on other formal Council events or formal UN processes. Only a few elected member states referred to less formal sources (such as past AFMs) as a way of promoting the discussion of an ICT topic.

[77] Although the growing use of AFMs may have hurt their significance (see *Report 1*).

Such future referencing remains an important measure of impact of Security Council events, however, since "building blocks" of common language constitute the basis of the Security Council's narratives and products. In the ICT track, which has so far predominantly featured AFMs, the limited impact in terms of future referencing therefore recalls the limitations that AFMs possess with regards to shaping discourse at the Security Council. Despite a growing number of events, the documents available for referencing in the ICT track remain low in the hierarchy of sources (except for one presidential statement). As interviewees pointed out, such common Security Council language is particularly needed when it comes to common definitions of ICT-related topics.

These findings related to framing and usage of expertise and sources are pertinent when considering ways forward in the ICT track. For instance, Estonia was able to foster some level of agreement around the otherwise contentious issue of cybersecurity by promoting a civilian perspective. This suggests that even in contentious areas, there are several possible pathways through which to utilise science-enhanced diplomacy. The "topic matrix" provided in this report maps issue areas in ICT over established UNSC agenda items, yielding in a number of salient topics at the intersection of ICT with protection of civilians, sustainable peace, efficiency of the UN, and others.

These areas can be further refined by applying alternative ways of tailoring topics as described in *Part 1: Leveraging Diplomacy with Science.* In doing so, an overall strategy could aim to leverage points of global consensus. For instance, attention to "consensus reports" by the GGE and OEWG, both UNGA First Committee bodies concerned with international norms and cybersecurity, is a useful way for Council members to draw on existing consensus at a global level (even if there also has been conflict around these groups). Points of convergence in other initiatives at the level of the General Assembly's Third Committee, such as ongoing negotiations for a Convention on Cybercrime (the Budapest Convention), can also be linked to, highlighting important collaboration around otherwise contentious issue areas. A further opportunity would be to leverage recent events with high salience in relation to these activity areas. For instance, recent events such as COVID-19 disinformation might be used to further underscore the importance of these issues if combined with a consensus-seeking framing.

Overall, this report has shown that in the early stages of a thematic track like the ICT, there are multiple ways that states can create opportunities for consensus. States should first determine whether their goal is to pursue a formal UNSC outcome or to support more generalized consensus-building, to determine whether it is more appropriate to develop a narrow topic framing that is bolstered with only formal sources, or to present a broader framing supported by a wider variety of expertise. They may, for instance, prefer a more explorative debate on the capabilities of certain technologies, even if it risks a less structured and more heated debate. Or they may foreground certain needs (including by the UN itself) that have potential technological solutions to them, which yields a less comprehensive but likely more productive debate related to ICT. The onus remains on states (especially the sponsors of an event) to decide between debates that explore new technologies more broadly but tend to be confrontational and debates that tend to be more productive but limited in scope and avoiding some of the most pressing issues.

The maintenance of international peace and security requires an understanding of the technologies and complex phenomena that shape international peace and security, whether

they come in the guise of risks or opportunities or both. While delegates may be individually supplied with knowledge through their capitals, it is crucial that the members of the Security Council progressively build up a shared language around emerging issues. To this end, the Security Council must be utilized as a forum for learning and knowledge dissemination on increasingly abstract matters. It would be deceiving, however, to advertise science and technological expertise as panacea to the challenges that the Security Council faces. As the Security Council faces challenges of increasing scientific and technological complexity, science itself risks becoming a tool in the rivalries among member states, rather than a solution to their disagreements. A responsible science-enhanced diplomacy is also about addressing those challenges in an attempt to open evidence- and analysis-based spaces for consensus-building and ultimately decision-making in the Security Council.

Appendix: Additional Details on the Topics Matrix

The following descriptions and accounts of topics and their relation to international peace and security give further details on topics mentioned in the Topics Matrix under three domains: protection of civilians, sustainable peace, and effectiveness of the UN. They are indicative only as informed by data within the scope of this project and are not intended to present an exhaustive account.

Protection of Civilians

+ *Cybersecurity: Protecting civilians against cyberattacks.*

Description: Malicious cyber activities that target civilians or critical civilian infrastructure can cause direct or indirect harm to civilians. Some experts also argue that cyberattacks on humanitarian actors are a matter of protection of civilians since humanitarians are meant to work on behalf of civilians in the context of conflict and often house sensitive data.[78]

- Prior discussion at the UNSC:
  - Closed AFM "Preventing Civilian Impact of Malicious Cyber Activities" (December 2021).
- Sensitivity: High due to high level of sensitivity around cybersecurity.

+ *AI / ML: Discrimination by AI/ML applications.*
  - Description: Artificial Intelligence and Machine Learning rely on large data sets, "with information about individuals collected, shared, merged and analysed in multiple and often opaque ways."[79]
  - Prior discussion at the UNSC:
    - Mentioned in May 2022 Briefing "The use of digital technologies in maintaining international peace and security."
  - Sensitivity: Medium-high given the overlap with questions of surveillance and data privacy.

+ *Emerging technologies (other) (1): Digital technology supporting humanitarian action (humanitarian corridors, demining, etc.).*
  - Description: Beyond cyber and digital threats, there are a variety of ways in which digital technologies can be leveraged to enhance the UN's work in the field. Existing initiatives like the Strategy for the Digital Transformation of UN Peacekeeping promote such applications.

[78] Interview #9.

[79] United Nations. 2021. "Urgent action needed over artificial intelligence risks to human rights." https://news.un.org/en/story/2021/09/1099972

- Prior discussion at the UNSC:
  - Digital opportunities such as drone corridors for the delivery of humanitarian supplies and the use of satellite data to map vulnerable populations at schools mentioned by UNICEF at Oct 2020 AFM.[80]
  - May 2022 Briefing.
- Sensitivity: Mid- to high sensitivity given potential links to the war in Ukraine, but could link to the positive response to Presidential Statement and Resolution on protecting peacekeepers (August 2021).

+ *Emerging technologies (other) (2): Access to education in conflict.*
  - Description: Without universal connectivity, the digital divide creates inequality in terms of access to education and opportunities. These divides are deepened in settings where infrastructure is damaged or schools become inaccessible.
  - Prior discussion at the UNSC:
    - Addressed by AFM (among primary topics): Oct 2020 AFM - digital technologies for distance learning; connectivity for all; public sector digitalisation [background COVID shutdowns]; this AFM possibly building off Sept 2020 press statement (S/PRST/2020/8 on attacks against schools and need to use digital tech to facilitate continuation of education during conflict
    - Examples cited by UNICEF at Oct 2020 AFM:[81]
      - Online framework for child safety
      - Connectivity bonds for internet access in vulnerable countries and communities hosting refugees [safe, universal connectivity]
      - Distance learning & online learning tools
      - Software for financial inclusion, health, education.
  - Further sources: On protecting education in conflict in general, see: Anna de Courcy Wheeler and Elizabeth Minor (2020): *Education and Conflict: Protecting Civilians and Protecting Education.* Article 36 Research Briefing.[82]
  - Sensitivity: Low

+ *Cryptocurrencies/Blockchain & FinTech: Financial technologies for unbanked crisis zones.*
  - Description: Large proportions of vulnerable populations are excluded from the financial sector: for instance, banks often retreat from conflict-affected regions, leaving them "unbanked," and refugees also lose access to banking services for numerous reasons. Money services based on mobile phone applications[83] can offer some remedy. Already in 2017, the World Bank's report on its *Global Findex Database* on financial inclusion noted that mobile money services provided an "important boost" in fragile and conflict-affected economies in Africa or in Haiti.
  - Prior discussion at the UNSC: N/A
  - Further sources:
    - Demirgüç-Kunt, Asli, Leora Klapper, Dorothe Singer, Saniya Ansar, and Jake Hess (2018): *The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution*. Washington, DC: World Bank. doi:10.1596/978-1-4648-1259-0.
  - Sensitivity: Medium. Whereas the topic *per se* should not be controversial, it is likely to be opposed by some member states (including P3) as soon as it appears to run counter to sanctions measures, measures to combat the financing of terrorism, and anti-money laundering policies.

+ *Social Media (1): Internet shutdowns to mask human rights violations.*
  - Description: These include state-enforced disruptions of internet service to control the flow of information, which can undermine the right to freedom of expression and also

[80] UNICEF. 2020. "Remarks by Henrietta Fore, UNICEF Executive Director, at Security Council meeting on universal connectivity and access to digital technology in conflict and post-conflict contexts." https://www.unicef.org/press-releases/remarks-henrietta-fore-unicef-executive-director-security-Council-meeting-universal.

[81] *Ibid.*

[82] De Courcy Wheeler, Anna and Elizabeth Miro. 2020. "Education and Conflict: Protecting Civilians and Protecting Education." *Article36.* https://reliefweb.int/report/world/education-and-conflict-protecting-civilians-and-protecting-education-august-2020.

[83] E.g., Amanacard. Online at: https:/../www.amanacard.com/ (accessed on 15.07.2022).

affect "anything from the right of people to contact relatives and loved ones during emergencies, to access health services, to digital assembly."[84]

- Prior discussion at the UNSC: N/A
- Further sources:
  - Office of the United Nations High Commissioner for Human Rights (2022): *Internet shutdowns: trends, causes, legal implications and impacts on a range of human rights* Report.
- Sensitivity: mid-to high given sovereignty and surveillance issues[85]

+ *Social Media (2): Access to information in conflict.*
  - Description: The right to access to information is listed as a fundamental right in the UN declaration of human rights (part of the right to the freedom of expression, Article 19). In conflict settings, there is a particular need to consider the different needs of different groups and to consider the UN's own role as an information actor.
  - Prior discussion at the UNSC:
    - "Access to education in conflict and post conflict contexts: Role of digital technology and connectivity" (October 2022 AFM).
  - Further sources:
    - Lahmann, Henning (2022): "Protecting the global information space in times of armed conflict," *International Review of the Red Cross* 915.
  - Sensitivity: Medium to high, as it relates to the practices of certain member states that engage in armed conflict and/or do not guarantee free access to media domestically.

Sustainable Peace

+ *Cybersecurity: Cyber and electoral security.*
  - Description: Cyberattacks (as well as social media and disinformation campaigns) have been used to intervene in elections abroad.
  - Prior discussion at the UNSC:
    - Briefly addressed during remarks at an AFM on "The Impact of Emerging Technologies" (May 2021).
    - Secondary topic in AFM "Artificial Intelligence: its impact on hate speech, disinformation and misinformation" (December 2023).
  - Sensitivity: High sensitivity due to past electoral interventions among permanent member states (e.g., alleged intervention of Russia into the 2016 US presidential elections).
+ *AI / ML: Deep fakes and other advanced disinformation and deception tools as risks to sustainable peace.*
  - Description: Deep fakes are realistic fake videos produced with AI/ML technologies that can involve politicians or other public figures and serve to misinform or agitate the public.
  - Prior discussion at the UNSC:
    - Link between AI and disinformation was addressed in AFM "Artificial Intelligence: its impact on hate speech, disinformation and misinformation" (December 2023).
  - Further sources: This was the object of a debate in the US congress, see: CNN: *Congress to investigate deepfakes as doctored Pelosi video causes stir* (4.6.2019).[86]
  - Sensitivity: Mid to high, to the extent it relates to the topic above (cyber and electoral security).

[84] United Nations Office of the High Commissioner for Human Rights. 2022. "Activists: Internet shutdowns violate human rights." https://www.ohchr.org/en/stories/2022/08/activists-internet-shutdowns-violate-human-rights#:~:text=Government%2Dimposed%20internet%20shutdowns%20cause,UN%20Human%20Rights%20Office%20warns.

[85] Interview #10.

[86] Archived at: https://web.archive.org/web/20190629081003/https://www.cnn.com/2019/06/04/politics/house-intelligence-committee-deepfakes-threats-hearing/index.html.

+ *Emerging technologies (other): Tech for good, tech for climate (big data, nanotech, biotech, quantum).*
    - Description: Tech for good is a loose term used to refer to a vast range of initiatives. This includes, for instance, the use of new technology to understand and address climate change or nanotech to support agriculture.
    - Prior discussion at the UNSC:
        + Addressed by AFM (secondary topic): Briefly addressed in "Impact of Emerging Technologies" AFM (May 2021), including potential use for understanding climate change (which can therefore help to address exacerbating factors: see end of Vincent Boulanin's expert briefing at the AFM and the subsequent response by the Chinese representative hosting the AFM).
    -
    - Sensitivity: Varies with precise topic but generally low. However, strong overlaps with development issues and the Sustainable Development Agenda mean that the Security Council's responsibility is likely to be contested by some member states.
+ *Cryptocurrencies/Blockchain & FinTech: Preventing corruption in public spending through e-procurement systems (optionally blockchain-based).*
    - Description: e-procurement systems can increase transparency of public spending, making a substantial contribution to the fight against corruption. These systems can make use of blockchain technology, albeit this is not required.
    - Prior discussion at the UNSC: In the October 2020 AFM on Education in conflict, UNICEF referenced the use of cryptocurrency for public services.
    - Further sources: Bustamante et al (2022): Government by Code? Blockchain Applications to Public Sector Governance, *Frontiers in Blockchain,* 21 June 2022, https://doi.org/10.3389/fbloc.2022.869665.
+ *Social Media (1): E-government / ICT for citizen empowerment & inclusion of women and youth in governance, mediation, and peacebuilding; bridging divided communities.*
    - Description: Digital technologies such as internet connectivity allows for wider inclusion in peace processes and governance.
    - Prior discussion at the UNSC:
        + Referenced in the briefing on New Technologies and International Peace and Security, May 22, 2022.
    - Sensitivity: Medium sensitivity, involving issues of transparent governance democracy, civil society, gender.
+ **Social Media (2):** *Hate speech & disinformation in social media*
    - Description: Violence attributed to online hate speech has increased globally, magnified by social media. Efforts to police inflammatory speech online are inconsistent, challenged by differing understandings of the role of tech companies and the implications on the freedom of expression. Hate speech is a known precursor conflict, sometimes escalating into genocide and other atrocities.
    - Prior discussion at the UNSC:
        + Primary topic of AFM "Hate speech and social media" (Oct 2021).
    - Further sources:
        + Kenyan concept note on the AFM "Hate speech and social media" (Oct 2021).
        + United Nations Strategy and Plan of Action on Hate Speech.[87]
    - Sensitivity: The AFM on this topic was closed, but an interviewee described it as an example of a more productive AFM. According to another interviewee, there is

[87] Online at: https://www.un.org/en/genocideprevention/hate-speech-strategy.shtml (accessed on 15.07.2022).

openness to discussing how mis/disinformation are shaping options in the ways that actors are pursuing conflict or peace.[88]

Effectiveness of the UN

+ *Cybersecurity: Protection of the UN secretariat and UN experts/investigators against cyberattacks.*
    - Description: Cybersecurity also matters for the UN. For instance, UN Panels of Experts members have reported insufficient technological equipment and training in earlier interviews with the authors of this report (in 2021).
    - Prior discussion at the UNSC: N/A
    - Further sources:
        + Joint Inspection Unit (2021) "Cybersecurity in the United Nations system organisations" https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2021_3_english.pdf.
    - Sensitivity: According to interviewees, the protection of UN staff and peacekeepers is a sensitive issue to the extent that cyberattacks typically stem from governments (mostly to gather information, not to sabotage). Therefore, framing these issues around the development of norms and standards of behaviour rather than immediate reaction to cyber incidents may be prudent.
+ *AI / ML: Efficiencies in UN Operations*
    - Description**:** AI and machine learning can help strengthen predictive analysis used in guiding decision making in UN operations or learning from mission performance. However, information gathering by UN operations remains contentious, with a continued need to clarify levels of accountability for possible harms.
    - Prior discussion at the UNSC:
        + Briefing "Artificial Intelligence: Opportunities and Risks for International Peace and Security" (July 2023).
    - Further sources:
        + Druet, Dirk (2021): Enhancing the use of digital technology for integrated situational awareness and peacekeeping-intelligence. Thematic Research Paper for the DPO Peacekeeping Technology Strategy
        + Strategy for the Digital Transformation of UN Peacekeeping
    - Sensitivity: Low for UNSC, but some debate on the ethics of information gathering during UN operations
+ *Cryptocurrencies/Blockchain & FinTech: Biometrics and software applications to register identities in refugee or displacement camps.*
    - Description: Digital identity platforms have been used by the UNHCR for refugees inside and outside camps (e.g., *PRIMES - Population Registration and Identity Management EcoSystem*). These platforms support the distribution of aid and allow refugees to have data such as their family relations and education acknowledged. Some critics argue that the potential of these tools remains underused, especially as it lacks integration with government services. The use of these technologies has the potential to promote effectiveness of UN operations in the field while also supporting the *protection of civilians* agenda.
    - Prior discussion at the UNSC: N/A.
    - Further sources:
        + Madon, Shirin (2021): Digital identity as a platform for improving refugee management. *Information Systems Journal 31 (6).* https://onlinelibrary.wiley.com/doi/10.1111/isj.12353.

[88] Interview #5.

    - Juskalian, Russ (2018): Inside the Jordan Refugee Camp that Runs on Blockchain. *MIT Technology Review, April 12 2018,* https://www.technologyreview.com/2018/04/12/143410/inside-the-jordan-refugee-camp-that-runs-on-blockchain/ (accessed on 14.7.2022).
  - Sensitivity: Low
- *Social Media: Transparency of UN activities; citizen engagement, information, and participation.*
  - Description: Social media, new communication tools, and other new interactive technologies facilitate a range of potential improvements to the Security Council´s efficiency as well as reforms to its working methods. These range from simpler outreach and communication measures in favour of heightened transparency to more complex proposals for citizen participation at the General Assembly and/or Security Council. While proposals of the latter kind face significant political objections, there are also less far-reaching measures. For instance, the Security Council's use of video conferences facilitates the participation of more diverse civil society briefers. Social media also presents opportunities for outreach related to peacekeeping missions.
  - Prior discussion at the UNSC: N/A.
  - Further sources:
    - Organ, James and Ben Murphy (2019): A Voice for Global Citizens: A UN World Citizen's Initiative. Democracy Without Borders, Democracy International, CIVICUS: World Alliance for Citizen Participation.
    - United Nations Peacekeeping (2021): Strategy for the Digital Transformation of UN Peacekeeping.
  - Sensitivity: Medium, as no major national interests are concerned, but diverging standards of transparent governance among member states are implied and some member states may object to debating such themes within the Security Council.