U.N Update: Cyber-Related Development

U.N. Update: Cyber-Related Developments in the Open-ended Working Group on security of and in the use of information and communications technologies (OEWG), Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (AHC), Global Digital Compact (GDC) and other U.N.-related discussions

GE-014
15 December 2023

ICANN

TABLE OF CONTENTS

INTRODUCTION **3**

OEWG UPDATE **4**

First substantive session 4
Second substantive session 9
Third substantive session 14
First Annual Progress Report of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025 16
Informal Consultations **17**
Forth substantive session 18
Fifth substantive session 18
U.N. Ad-hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (AHC) **20**
First session (submissions related to the first session of the AHC) 20
Second session (submissions related to the second session of the AHC) 21
Third session (submissions related to the Third Session of the AHC) 23
Fourth and Fifth sessions of the AHC. 25
Sixth session of the AHC. 26

GLOBAL DIGITAL COMPACT AND THE SUMMIT OF THE FUTURE **32**

Introduction/Background **32**
The Global Digital Compact **32**
Other UN Initiatives 38
Conclusion **39**

Introduction

This paper provides an update on the proceedings of the United Nations General Assembly (UNGA), where discussions of cyber-related issues take place. It includes updates from the deliberations at the second Open-Ended Working Group (OEWG)[1] and the Ad Hoc Committee of Experts (AHC)[2] between 4 June 2021 and 2 September 2023 as well as more recent discussions on and around the Global Digital Compact in 2023.

As one of a periodic series of reports, this paper provides an overview of activities taking place at the U.N. that are relevant to the Internet ecosystem and to the mission of the Internet Corporation for Assigned Names and Numbers.[3] Monitoring such activities demonstrates the commitment and responsibility of the ICANN organization's (org) Government and Intergovernmental Organization Engagement (GE) team to keep the broader ICANN community informed about issues of importance for the global, single, interoperable Internet and its unique identifier system.[4]

[1] Open-ended Working Group on security of and in the use of information and communications technologies (OEWG), https://meetings.unoda.org/meeting/57871/statements
[2] Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home
[3] See previous reports by GE here: https://www.icann.org/en/government-engagement/publications This and all other URLs in footnotes and appendices were retrieved on [insert] August 2023.
[4] "ICANN Operating and Financial Plans," p. 47, ICANN organization, December 2020, https://www.icann.org/en/system/files/files/draft-op-financial-plan-fy21-25-opplan-fy21-20dec19-en.pdf

OEWG Update

First substantive session[5]

9 December 2021

China: “The current distribution and management system of critical Internet resources is imbalanced and unjust.” [...] “States should participate in the management and distribution of international Internet resources on equal footings, and build a global Internet governance system of multilateralism, democracy and transparency.”[6]

12 December 2021

China: “the States have the right to exercise, in accordance with the universally recognized principles and rules of international law, necessary and reasonable personal, territorial and protective jurisdiction over specific ICT activities outside their territories that have genuine and substantial connection to the States as well as over relevant ICT-related facilities, entities, data and information. In order to exercise its jurisdiction, a State may seek assistance from other States and regions in the spirit of self-restraint, comity and reciprocity.”
[...]
“Manifestation of Sovereignty in the Physical Layer. States have jurisdiction over the physical infrastructure and basic ICT services within their territories. States are entitled to take necessary measures to maintain the security of the physical infrastructure according to national law and in conformity with international law. States have the right to participate in the management of and international cooperation on the global Internet infrastructure.” [...] “Manifestation of Sovereignty in the Logical Layer. States can independently enact or adopt the relevant technical regulations or standards while maintaining the interoperability of the Internet in accordance with their obligations under international law.”[7]

Context: In a recent white paper issued by the State Council Information Office of the People’s Republic of China, the following points on governance and critical Internet resources are worth quoting:

“Chapter III, Point #3: Actively Participating in Cyberspace Governance
China has actively participated in the operation of global internet organizations. It has actively participated in the activities of platforms and organizations such as the Internet Corporation for Assigned Names and Numbers (ICANN). It has supported reform of the ICANN governance mechanism to increase the representation of developing countries, and to bring more Internet information resources under concerted global management. China has also participated in the activities of the Internet Society (ISOC), Internet Engineering Task Force (IETF), and Internet Architecture Board (IAB). It has played a constructive role in facilitating community exchange,

[5] The quotes from the OEWG and AHC sessions include both written and oral statements
[6] China’s Views on the Application of the Principle of Sovereignty in Cyberspace, December 9 2021, p. 1, https://documents.unoda.org/wp-content/uploads/2021/12/Chinese-Position-Paper-on-International-Rules-making-in-Cyberspace-ENG.pdf
[7] China’s Views on the Application of the Principle of Sovereignty in Cyberspace, 12 December 2021, pp. 1 and 4, https://documents.unoda.org/wp-content/uploads/2021/12/Chinese-Position-Paper-on-the-Application-of-the-Principle-of-Sovereignty-ENG.pdf

promoting technical R&D and application, and becoming closely involved in the formulation of relevant standards and rules."
[...]

Chapter IV, Point #5: 5. Maintaining the security and stability of the core-resource management system for the internet
The core-resource management system for the internet is the cornerstone of internet operations. It should be guaranteed that those institutions hosting the management systems operate with full credibility and do not pose a threat to the top-level domains of any country just because of the jurisdictional demands on some other country. China advocates guaranteed availability and reliability of core internet resources – to be used by all countries and jointly managed and fairly distributed by the international community, so that the technological systems for the resources, including the domain name system, are secure, stable, and resilient. There should be a guarantee that services will not be interrupted or terminated due to any political or human factors. China advocates that governments, industry authorities, and businesses work together to accelerate the use of IPv6 technology and applications."[8]

[8] Xinhua, China issues white paper on community with shared future in cyberspace, November 7, 2022 https://english.www.gov.cn/archive/whitepaper/202211/07/content_WS636894aac6d0a757729e2973.html

14 December 2021

Portugal: “A strong international cooperative effort in the resilience of the national critical infrastructures of all UN member states and of the Internet core that binds them all together carried out in compliance with human rights, international law and according to the highest benchmarks is essential to deter cyber attacks below the threshold of armed conflict.”[9]

China: “The future of the internet should not and cannot possibly be controlled by a handful of countries. Forming ideologically exclusive small circles and clinging on to ICT monopoly and cyber harmony will only hinder multilateral efforts to promote cyber security. Certain countries have sought to launch the so-called “alliance for future of the internet” which is nothing but the example of attempts to divide the internet, seek technology monopoly and cyberspace hegemony and suppress the science and technology development of other countries only to serve their own geopolitical agenda. They claim to build an open internet, but in fact are stirring up confrontation and dividing the internet, which completely runs counter to [the] internet spirit of peace, security, openness and cooperation, and the common interest of [the] international community.”[10]

“Meanwhile, we should, in line with the attributes of ICTs and the needs of [the] evolving situation, discuss the formulation of new norms. Data Security is a prominent new challenge facing all countries. Based on the mandate of the resolution, parties would hold in-depth discussions on issues of cross border data flow, supply chain security, and personal information protection, and explore appropriate responses. China’s Global Initiative on Data Security could serve as a preliminary basis for discussion.”[11]

Context: In the same statement, there is criticism of initiatives by other countries and a proposal for China’s own “Initiative on Data Security” that “could serve as a preliminary basis for discussion.”

Spain: “If we cannot manage to agree on global regulations within the United Nations current geopolitical tensions could lead to a fragmentation of cyberspace into various areas of influence with standards certification and technical specificities which are incompatible with each other.”[12]

China: “Cyberspace is at risk of fragmentation. UN Secretary General Gutierrez warned during this year's General Assembly that the world is at risk of splitting in two with two conflicting sets of standards. The same is true of cyberspace.”[13]

---

[9] UN Web TV, 3rd plenary meeting, Open-ended working group on security of and in the use of information and communications technologies 2021–2025 – First substantive session, 14 December 2021, https://media.un.org/en/asset/k11/k11eljcg88 (starts at 1:14:20)

[10] UN Web TV, 3rd plenary meeting, Open-ended working group on security of and in the use of information and communications technologies 2021–2025 – First substantive session, 14 December 2021, https://media.un.org/en/asset/k11/k11eljcg88 (starts at 1:50:40)

[11] Statement by Counsellor Wu Jianjian, Head of the Chinese Delegation at the General Exchange of Views of the First Substantive Session of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies, 14 December 2021, https://documents.unoda.org/wp-content/uploads/2021/12/Statement-of-China_ICT-OEWG-3rd-plenary-meeting_General-Exchange-of-Views_DEC-14-AM_ENG.pdf

[12] UN Web TV, 4th plenary meeting, Open-Ended working group on security of and in the use of information and communications technologies 2021–2025 – First substantive session, 14 December 2021, https://media.un.org/en/asset/k1b/k1b55qgp81 (starts at 04:30)

Islamic Republic of Iran: “This requires a more comprehensive approach to threats in the sphere of information security which addresses not only the digital infrastructure but also the content and information itself. Some examples of urgent and challenging, existing and potential threats that states are facing are as follows: (1) monopoly and hegemony in the Internet governance…”[14]

Context: There is no evidence of any “monopoly and hegemony” in Internet governance. Internet governance has been discussed widely at the WSIS and during the WSIS+10 negotiations at the U.N. General Assembly, and no such conclusion has been reached in the WSIS Tunis Agenda or the WSIS+10 Outcome Document.

15 December 2021

The Netherlands: “Some examples of existing challenges and potential threats that the global community is facing include cyber operations against the integrity, functioning and availability of the internet, as referred to in the acquis. This technical infrastructure essential to the general availability or integrity of the internet, or the public core, was referred to on critical infrastructure in both the previous OEWG and GGE reports (norm 13f). This technical infrastructure essential to the general functioning of the internet also needs protection against tendencies to control it in a way that would undermine the integrity or availability of the internet. We see these tendencies coming from a broad range of actors. In particular, the Internet governance model, which is based on multistakeholder governance, should in no way be undermined. The private sector, civil society, technical community and other stakeholders are indispensably connected to the functioning of the Internet.”[15]

Islamic Republic of Iran: “We are of the view that significant reforming of the current Internet governance, open fair and nondiscriminatory access of states to ICT technologies and reliable cyber-security supply chain are essential requirements of responsible behavior of states in the ICT environment”.[16]

Context: The Working Group on Internet Governance (WGIG) developed this definition of Internet Governance: "Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the

[13] UN Web TV, 4th plenary meeting, Open-ended working group on security of and in the use of information and communications technologies 2021–2025 – First substantive session, 14 December 2021, https://media.un.org/en/asset/k1b/k1b55qgp81 (starts at 1:56:42)
[14] UN Web TV, 4th plenary meeting, Open-ended working group on security of and in the use of information and communications technologies 2021–2025 – First substantive session, 14 December 2021, https://media.un.org/en/asset/k1b/k1b55qgp81 (starts at 2:35:20)
[15] UN Web TV, 5th plenary meeting, Open-ended working group on security of and in the use of information and communications technologies 2021–2025 – First substantive session, 15 December 2021, https://media.un.org/en/asset/k1r/k1royetcr4 (starts at 39:42), also here: Statement by H.E. Nathalie Jaarsma, Ambassador at-Large for Security Policy and Cyber, 15 December 2021, https://documents.unoda.org/wp-content/uploads/2021/12/21.12.15-Netherlands-Statement-on-Threats-OEWG-in-the-Field-of-Information-and-Telecommunications-in-the-Context-of-Internat.pdf
[16] UN Web TV, 6th plenary meeting, Open-ended working group on security of and in the use of information and communications technologies 2021–2025 – First substantive session, 15 December 2021, https://media.un.org/en/asset/k1r/k1rnexulnt (starts at 50:35)

Internet."[17] Accordingly, it does not pertain to the issues in the statement. The current state of Internet governance is discussed every year at the Internet Governance Forum (IGF), which is the appropriate venue for such discussions because it is open to anyone to participate. The future state of Internet governance will be discussed during WSIS+20 in 2025, at the U.N. General Assembly.

India: "We need to discuss the obligations for non-conducting and knowingly allowing attacks upon the public core of the Internet. That includes: package routing, and forwarding elements, naming and numbers systems, the cryptographic mechanisms of security and identity, transmission media, software and data centers".[18]

16 December 2021

Costa Rica: "Best practices and lessons could also be drawn from the technical community, as CERTs have led communities that rely on trusted relationships to exchange information to respond to ICT events. We can draw lessons on the importance of going beyond merely listing names in a directory, but rather convening meetings or conducting exercises to build trust and relationships within the network."[19]

17 December 2021

Islamic Republic of Iran: "The OEWG should address the main sources of mistrust in the ICT environment, particularly the monopoly in the internet governance, anonymity, offensive cyber strategies, hostile image-building and xenophobia leading to unilateral coercive measures, and lack of responsibility of private companies and platforms and their national states for extraterritorial activities. For example, the departure point is to realize multilateral, fair, and transparent internet governance."[20]

Context: There is no evidence of a "monopoly in Internet governance." Internet governance is defined within the WSIS Tunis Agenda and all stakeholders including governments participate in it. Neither is there a proven consensus for a new, multilateral model of Internet governance. This much was stated by Germany on 28 March 2022 (see quote below).

[17] Report of the Working Group on Internet Governance, June 2005, point 10, https://www.wgig.org/docs/WGIGREPORT.pdf

[18] UN Web TV, 6th plenary meeting, Open-ended working group on security of and in the use of information and communications technologies 2021–2025 – First substantive session, 15 December 2021, https://media.un.org/en/asset/k1r/k1rnexulnt (starts at 01:48:55)

[19] UN Web TV, 8th plenary meeting, Open-ended working group on security of and in the use of information and communications technologies 2021–2025 – First substantive session, 16 December 2021, https://media.un.org/en/asset/k1y/k1yzr8yhb1 (starts at: 57:20), also here: Permanent Mission of Costa Rica to the United Nations, statement, 16 December 2021, https://documents.unoda.org/wp-content/uploads/2021/12/Final-Costa-Rica-CBMs-1612021-SP-EN.pdf

[20] Submission to the First Substantive Session Iran (Islamic Republic of), 17 December 2022, p. 8-9, https://documents.unoda.org/wp-content/uploads/2021/12/Irans-submission-to-first-substantive-session_13-17-Dec-21.pdf

Second substantive session

28 March 2022

U.N. Under-Secretary-General Izumi Nakamitsu: “It is universally recognized – multi-stakeholder engagement is essential in the area of ICT security where private actors own and manage much of the relevant infrastructure.”[21]

USA: “This [OEWG] process here today [...] belongs to every member state that seeks to preserve stability in cyberspace, it belongs to every stakeholder that benefits from an open, interoperable, secure and reliable Internet for all...”[22]

Germany: “The Internet is neither owned nor controlled by states. It is a public domain which is managed and advanced by a highly complex and efficient range of actors representing industry, civil society and government. The participation in this Open Ended Working Group should be fully reflective of this reality.”[23]

Spain: “We see the true threat of fragmentation within spheres that could affect technical specifications that might end up being entirely incompatible amongst themselves. We cannot allow for this to occur because it will directly affect all of our countries.”[24]

29 March 2022

Russian Federation: “For example, there is an absolutely real possibility of an entire country being cut off from the international communications systems, in particular from the Internet, or the interbank system for carrying information and making payments, SWIFT. It is not a theoretical threat; it is what is happening to my country. Experience shows that technology makes it possible to carry out this threat, as these systems are managed by one country or a very small group of countries. And so, taking the Internet as an example, this would be the corporation for managing domain names and IP addresses, ICANN. It is an international non-profit organization, which de facto is fully controlled by the United States of America. These conditions make any country - any! - vulnerable to the political decisions of such a country.”[25]

---

[21] UN Web TV, (1st meeting) Open-ended working group on security of and in the use of information and communications technologies 2021–2025, Second substantive session, March 29 2022, https://media.un.org/en/asset/k1h/k1hhzc7i5z (starts at 6:27)

[22] UN Web TV, (1st meeting) Open-ended working group on security of and in the use of information and communications technologies 2021–2025, Second substantive session, March 29 2022, https://media.un.org/en/asset/k1h/k1hhzc7i5z (starts at 35:00)

[23] UN Web TV, (1st meeting) Open-ended working group on security of and in the use of information and communications technologies 2021–2025, Second substantive session, March 29 2022, https://media.un.org/en/asset/k1h/k1hhzc7i5z (starts at 1:13:55), and also here: German Statement at the March OEWG, Agenda Item 3, 22 April 2022, p. 3, https://documents.unoda.org/wp-content/uploads/2022/04/German-Statement-at-the-March-2022-OEWG-Agenda-Item-3.pdf)

[24] UN Web TV, (1st meeting) Open-ended working group on security of and in the use of information and communications technologies 2021–2025, Second substantive session, March 29 2022, https://media.un.org/en/asset/k1h/k1hhzc7i5z (starts at 1:52:38)

[25] UN Web TV, (3rd meeting) Open-ended working group on security of and in the use of information and communications technologies 2021–2025, Second substantive session, 29 March 2022, https://media.un.org/en/asset/k1l/k1l7rcax4f (starts at 51:05)

Context: ICANN is not in a position to "cut off" (stop, shut down, etc.) any country from the Internet. This is stated quite clearly in a letter dated 2 March 2022, from ICANN's President and CEO in response to the Ukrainian Deputy Prime Minister.[26] The Regional Internet Registry for Europe, the Middle East and parts of Central Asia, RIPE Network Coordination Center (RIPE NCC) expressed a similar position in a publication dated March 10, 2022.[27] This was also noted on 5 April 2022, when Ms. Fiona Alexander[28] said: "The Russian Federation was better protected in the multistakeholder model than it has been in the U.N. system. So, while the Ukrainian minister asked both RIPE and ICANN to take away their Internet resources, both said "no."[29] But in March 2022, in the ITU World Telecom Standardization Assembly, the Russian government was stripped of leadership positions in the study groups at the request of Ukraine.[30] So, even though the Russian Federation participates in ICANN, [it] wants to have it taken over by the ITU or replaced. It was ironic to me that the multistakeholder model actually better protected the people of Russia and the Internet than the U.N. system, where the Russian government was actually stripped of its role."[31] On 6 April 2022 the White House issued a fact sheet on U.S., G7, and EU sanctions on Russia, in which it states that access to the Internet is not a target of the sanctions.[32]

Malaysia: "In this regard [we] might consider swift and effective measures by hosting provider and enforcement entities, Internet service providers, domain name registrars in blocking and takedown of malicious sites at the level of hosting provider need to be focused on, especially those that affect the critical information infrastructure."[33]

Netherlands: "Initiatives that harm the technical infrastructure essential to the general availability or integrity of the Internet also referred to as the public core of the Internet, include cyber operations that target the core physical and logical infrastructure of the Internet, or the organizations that are central to global routing, naming and numbering, such as regional Internet registries, ICANN and large Internet exchanges. They also include those that introduce

[26] Letter from Göran Marby, President and CEO, Internet Corporation for Assigned Names and Numbers (ICANN) to Mykhailo Fedorov, Deputy Prime Minister, Minister of Digital Transformation Ukraine, 2 March 2022, https://www.icann.org/en/system/files/correspondence/marby-to-fedorov-02mar22-en.pdf

[27] RIPE NCC, RIPE NCC Response to Request from Ukrainian Government, 10 April 2022, https://www.ripe.net/publications/news/announcements/ripe-ncc-response-to-request-from-ukrainian-government

[28] Fiona Alexander is currently a Distinguished Policy Strategist in Residence in the School of International Service and Distinguished Fellow at the Internet Governance Lab at American University. For close to 20 years, Fiona served at the National Telecommunications and Information Administration (NTIA) in the U.S. Department of Commerce where she was Associate Administrator for International Affairs.

[29] RIPE NCC Response to Request from Ukrainian Government Letter from the Vice Prime Minister of Ukraine to RIPE NCC (PDF), Response from Managing Director of the RIPE NCC (PDF), Amsterdam, 10 March 2022, https://www.ripe.net/publications/news/announcements/ripe-ncc-response-to-request-from-ukrainian-government

[30] Official Twitter account of the Permanent Mission of Ukraine to the U.N. Office in Geneva, 9 March 2022, https://twitter.com/UKRinUNOG/status/1501658319932600326, Website of the Permanent Mission of the Czech Republic to the U.N. Office in Geneva, 9 March 2022, https://www.mzv.cz/mission.geneva/en/specialized_agencies/international_telecommunication_union/russia_s_military_aggression_against.html

[31] Fiona Alexander, ITIF webinar, Internet Governance During Times of War and Conflict, 5 April 2022, (starts at 58:57), https://itif.org/events/2022/04/05/internet-governance-during-times-war-and-conflict

[32] The White House, Briefing Room, FACT SHEET: United States, G7 and EU Impose Severe and Immediate Costs on Russia, 6 April 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/06/factsheet-united-states-g7-and-eu-impose-severe-and-immediate-costs-on-russia/

[33] UN Web TV, (3rd meeting) Open-ended working group on security of and in the use of information and communications technologies 2021–2025, Second substantive session, 29 March 2022, https://media.un.org/en/asset/k1l/k1l7rcax4f (starts at 1:18:48)

Internet standards and protocols that undermine the open and interoperable character of the Internet. To further deepen our technical understanding of the public core the Netherlands will initiate activities on the public core to deepen our joint technical understanding among this Open-ended Working Group community."[34]

Islamic Republic of Iran: "Notwithstanding the risks emanating from the existing monopoly in internet governance and the need for a new architecture, this issue has not yet been effectively discussed in the United Nations system since the World Summit on the Information Society (WSIS) held in in Tunis in 2005 (Articles 29 to 82 of the Tunis Agenda for the Information Society). It is unfortunate that the Internet Governance Forum (IGF) refuses to discuss this issue and refers it to the OEWG while the OEWG considers it beyond its mandate to discuss internet governance and refers it to the IGF. As a result, the international community was unable to achieve a consensus with regard to the global governance of the internet which would thereby remove the current monopoly over the governance of the internet. The international community must outline a better solution for internet governance within the OEWG shortly which will safeguard the stability and security of the ICTs environment." [35]

Context: Here again, as earlier in the week, Iran claims that there is an "existing monopoly in Internet governance," which is a view that is not supported by facts. Further, Iran claims that there is a need for "a new architecture," but it's not clear what this "new architecture" would be. However, the issue of improvements to the digital cooperation architecture was addressed in the UN Secretary General's Roadmap for Digital Cooperation. In 2022, the U.N. the Secretary General established the IGF High Level Leadership Panel, a multistakeholder body to support and strengthen the IGF.[36] Furthermore, all issues related to Internet governance have been discussed since 2003 within the WSIS and the WSIS+10 review as well as, on a number of occasions, at the IGF. Iran claims that the IGF "refuses to discuss this issue," but the IGF is actively discussing any issues that participants have put forth in the form of proposals, which have been accepted by the IGF Multistakeholder Advisory Group. Internet governance is global, and well described and explained in the WSIS documents.[37]

France: "My delegation would like to draw the attention of the Group to the threats to free and interoperable nature of cyberspace. In the context of the international attention we could see an increasing siloing of cyberspace [...] including at the very deepest levels. [...] There has never been sanctions with regard to states accessing deep levels of the Internet. But this temptation is discussed increasingly and is very dangerous. This fragmentation brings with it risks not just for the respective human rights, to the free circulation of information, economic growth, but

[34] UN Web TV, (3rd meeting) Open-ended working group on security of and in the use of information and communications technologies 2021–2025, Second substantive session, 29 March 2022, https://media.un.org/en/asset/k1l/k1l7rcax4f (starts at 1:26:20)

[35] UN Web TV, (3rd meeting) Open-ended working group on security of and in the use of information and communications technologies 2021–2025, Second substantive session, 29 March 2022, https://media.un.org/en/asset/k1l/k1l7rcax4f (starts at 1:35:05), and also here: Statement by Delegation of the Islamic Republic of Islamic Republic of Iran To the Second Substantive Session of the Open-ended Working Group on security of and in the use of information and telecommunications technologies, 29 March 2022, p. 3, https://documents.unoda.org/wp-content/uploads/2022/03/1-Introductory-Remarks-Existing-and-Potential-Threats.pdf

[36] Also see, United Nations, Secretary-General's High-level Panel on Digital Cooperation, https://www.un.org/en/sg-digital-cooperation-panel

[37] Leadership Panel & Multistakeholder Advisory Group Joint Letter to GDC Co-Facilitators, "The United Nations' Internet Governance Forum stands ready to accept the responsibilities arising from the Global Digital Compact periodic multistakeholder review and follow-up", 16 October 2023, https://www.intgovforum.org/en/filedepot_download/24/26649

increasingly for international stability. Indeed, if we have several different Internets, states might decide to engage in malevolent activities if they feel they could do this by protecting the precarious Internet, and having another one in addition to that. Our group should take account of this and it should lead us to redouble our efforts to preserve the architecture of the free cyberspace that is singular, open, stable, safe and universally accessible."[38]

30 March 2022

The Netherlands: "For the Netherlands, safeguarding the public core includes respecting its multistakeholder governance model, and preventing the introduction of standards and protocols that would undermine the open and interoperable nature of the Internet. In this context, and in reaction to what was suggested yesterday, I would like to highlight that the role of the multistakeholder organizations like ICANN and Regional Internet Registries is to ensure the technical coordination of the Internet and work to uphold a single, global and interoperable Internet, that continues to operate at all times, and is accessible to all…"[39]

Russian Federation: "All states should play an equal role in the international Internet governance and bear equal responsibility for Internet governance."[40]

Context: There is no evidence that states do not play an "equal role in the international Internet governance," nor that they do not "bear equal responsibility" for it.

China: "We are of the view – that states have jurisdiction over the ICT infrastructure, resources as well as activities on their territories. No country should sabotage the critical infrastructure of other states with ICT or engage in the destruction or theft of the important data of such infrastructure. States should improve the legislation on the protection of CII" [...] "From September 1 2021 China's regulation on protecting the security of critical information infrastructure came into effect. According to the regulation critical information infrastructure is defined as important networks and information systems of key industries and sectors, such as public telecommunication and information services, energy, transportation, hydraulic works, finance, public service, e-government and defense, science and technology. And while there are others such networks and systems whose compromise, loss of function or data breach may seriously jeopardize national security, national economy and public interests. China welcomes in-depth discussions at the OEWG on the definition and protection of critical infrastructure based on the principle of sovereignty."[41]

---

[38] UN Web TV, (3rd meeting) Open-ended working group on security of and in the use of information and communications technologies 2021–2025, Second substantive session, 3rd meeting, 29 March 2022, https://media.un.org/en/asset/k1l/k1l7rcax4f (starts at 15:07)

[39] UN Web TV, (5th meeting) Open-ended working group on security of and in the use of information and communications technologies 2021–2025, Second substantive session, 30 March 2022, https://media.un.org/en/asset/k1g/k1gu15nuh2 (starts at 1:00:07)

[40] UN Web TV, (5th meeting) Open-ended working group on security of and in the use of information and communications technologies 2021–2025, Second substantive session, 30 March 2022, https://media.un.org/en/asset/k1g/k1gu15nuh2 (starts at 1:10:18) and also here: Statement by the Head of the Russian Federation Delegation V. Shin, 30 March 2022, p. 3, https://documents.unoda.org/wp-content/uploads/2022/03/Russia-OEWG-statement-3-30.03.2022-Eng.pdf)

[41] UN Web TV, (5th meeting) Open-ended working group on security of and in the use of information and communications technologies 2021–2025, Second substantive session, 30 March 2022, https://media.un.org/en/asset/k1g/k1gu15nuh2 (starts at 1:57:29)

Portugal: “IP manipulation in the context of attacks against the Internet core or against the integrity of electoral processes can also be paramount.”[42]

Singapore: “One example of critical infrastructure could be the technical infrastructure systems essential to the general availability or integrity of the Internet.” [43]

Russian Federation: “At the current stage of the ICT development unmistakably identifying the source of harmful activity does not appear to be possible without an in-depth reform of the protocols of the functioning of the global communication network and organizing the necessary cooperation between states. In this regard establishing a clear mechanism of cooperation between authorized state bodies along the lines of CERT-to-CERT cooperation is highly relevant.”[44]

Context: There is no evidence that such an “in-depth reform of the [Internet]” is needed for the stated purpose. Around the world, there are countless criminal cases where law enforcement was able to identify the source of the described activity.[45]

31 March 2022

Canada: “For example, at the OSCE, we are championing CBM 4, along with Kazakhstan. It aims to promote information sharing on national approaches to ensure an open, secure, interoperable internet. This work will hopefully help protect the general availability and integrity of the internet, an objective shared by The Netherlands and others who have mentioned it this week.”[46]

Islamic Republic of Iran: “Trust and confidence-building measures in cyberspace (TCBMs) shall be built into an ICT environment to address the main sources of mistrust in the ICT environment, particularly the monopoly in internet governance, anonymity, offensive cyber strategies and policies, hostile image-building and xenophobia, unilateral coercive measures, and the lack of responsibility of private companies as well as platforms and their respective states for extraterritorial activities.

---

[42] UN Web TV, (5th meeting) Open-ended working group on security of and in the use of information and communications technologies 2021–2025, Second substantive session, 30 March 2022, https://media.un.org/en/asset/k1g/k1gu15nuh2 (starts at 2:06:50)

[43] UN Web TV, (5th meeting) Open-ended working group on security of and in the use of information and communications technologies 2021–2025, Second substantive session, 30 March 2022, https://media.un.org/en/asset/k1g/k1gu15nuh2 (starts at 2:36:05)

[44] UN Web TV, (6th meeting) Open-ended working group on security of and in the use of information and communications technologies 2021–2025, Second substantive session, 30 March 2022, https://media.un.org/en/asset/k1j/k1jpaw8mgf (starts at 34:40)

[45] See the Russian Federation Ministry of Internal Affairs (MVD) Report on the State of Crime in Russia for the period between January and November 2022, p. 3, point 9. https://d-russia.ru/wp-content/uploads/2022/12/mvd_22_11_.pdf or the 2022 FBI Internet Crime Report, p. 8, https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf or Crime in India, Ministry of Home Affairs, National Crimes Records Bureau, India, TABLE 9A.2 Cyber Crimes - IT Act Cases (Crime Head-wise & State/UT-wise) - 2021, https://ncrb.gov.in/uploads/nationalcrimerecordsbureau/post/1679661922TABLE9A2.pdf

[46] UN Web TV, (7th meeting) Open-ended working group on security of and in the use of information and communications technologies 2021–2025, Second substantive session, 31 March 2022, https://media.un.org/en/asset/k1i/k1iykegjsm (starts at 22:40)

We believe that the departure point is to realize multilateral, fair and transparent internet governance. We are of the view that the monopoly (in management) and anonymity (of persons and things) are the main sources of mistrust on the internet, which necessitates relevant CBMs. The first and foremost approach is to address the shortcomings and downsides of the current internet governance system with a view to realizing long awaited fair internet governance."[47]

Third substantive session

25 July 2022

Under-Secretary-General Izumi Nakamitsu: "I welcome the proposals related to strengthening the protection of critical infrastructure and critical information infrastructure including through enhanced interactions with interested stakeholders on this topic. This is in line with cause by the Secretary General for prioritization on measures that enhance the protection of critical infrastructure including the health sector."[48]

And: "I have repeatedly emphasized the importance of engaging stakeholders in an inclusive and sustained manner given the unique nature of ICTs and the central role played by non-governmental entities in the management of many ICT resources."[49]

European Union: "The list includes also controversial elements. First the proposal to agree on the terminology and the list of critical infrastructure is an example of a proposal that in our experience would not allow for a consensus discussion between states. Based on experiences in prior multilateral and regional settings these discussions are considered divisive, time-consuming and could imply in the case of the list of critical infrastructure that they are acceptable targets."[50]

China: "In reality, regarding the trend of how the ICT environment is becoming more and more divided, I believe other colleagues present here are aware of this trend and reality. U.N. Secretary General Guterres in two successive general debates of the U.N. General Assembly has reminded the international community of the threat of the ICT environment becoming, cyberspace becoming more and more fragmented. So, the fragmentation of the ICT environment is directly related to our deliberations. So, if this world is divided or fragmented into different parts, then no single set of rules would apply. Then it would be impossible for us to reach consensus on the implementation or applicability of international rules. Let alone any confidence building measures. So, I hope under part of existing and potential threats we need to

[47] UN Web TV, (7th meeting) Open-ended working group on security of and in the use of information and communications technologies 2021–2025, Second substantive session, 31 March 2022, https://media.un.org/en/asset/k1i/k1iykegjsm (starts at 31:50), and also here: Statement by Mr. Heidar Ali Balouji, First Counselor, Permanent Mission of the Islamic Republic of Iran to the United Nations, 31 March 2022, p. 1, https://documents.unoda.org/wp-content/uploads/2022/03/4-CBMs.pdf

[48] UN Web TV, (1st meeting) Open-ended working group on security of and in the use of information and communications technologies 2021–2025, Third substantive session, 25 July 2022, https://media.un.org/en/asset/k1u/k1uo46thhm (starts at 5:53)

[49] UN Web TV, (1st meeting) Open-ended working group on security of and in the use of information and communications technologies 2021–2025, Third substantive session, 25 July 2022, https://media.un.org/en/asset/k1u/k1uo46thhm (starts at 7:54)

[50] UN Web TV, (1st meeting) Open-ended working group on security of and in the use of information and communications technologies 2021–2025, Third substantive session, 25 July 2022, https://media.un.org/en/asset/k1u/k1uo46thhm (starts at 2:07:34)

include some deliberations on how to tackle the most important, most prominent issue in the ICT environment right now."[51]

Spain: **"**When it comes to cyber-threats we propose that the report describe these reflecting the existing problems in cyberspace and the problems that they imply for the working of digital society, private citizens and the working of state institutions through technical and standard-setting, effective protection of personal data should be insured as well as intellectual property in transboundary and international exchanges. We have a General Data Protection Regulation in Europe which sets high levels of stability and security in the exchange of data. The safer, the greater these guarantees of protection are – the greater the protection there will be and the greater the willingness there will be for the citizens and businesses to exchange data."[52]

Brazil: **"**Finally on point of interfaces, -- there is an interface in the report with the Internet governance track, when we discuss risks of fragmentation, ensuring availability and integrity: we welcome this concern in the report but we would like to be mindful of the proper place to discuss broader Internet governance issues."[53]

Russian Federation: "It is principal to reflect in the zero-draft report the measures on accessibility of secure and stable functioning of the Internet with the stress on the sovereignty of the states in their respective national information space. And securing the equal participation of the states in managing this network."[54]

Context: State participation in Internet governance is an issue that has been discussed and resolved during the WSIS. The global Internet consists of thousands of connected networks that are independently owned and managed - some of them by governments.There is no evidence that states do not have the right to "equal participation… in managing this network."

Russian Federation: "On strengthening the interaction with non-governmental subjects in the business of ICT security we see an advantage in hearing the opinion of those interested parties that bear direct responcibility in defending the object of critical infrastructure, including critical information infrastructure, being its subjects. Such a dialogue should take place with the understanding of the key role of national governments in this issue."[55]

---

[51] UN Web TV, (1st meeting) Open-ended working group on security of and in the use of information and communications technologies 2021–2025, Third substantive session, 25 July 2022, https://media.un.org/en/asset/k1u/k1uo46thhm (starts at 2:26:14)

[52] UN Web TV, (1st meeting) Open-ended working group on security of and in the use of information and communications technologies 2021–2025, Third substantive session, 25 July 2022, https://media.un.org/en/asset/k1u/k1uo46thhm (starts at 2:41:52)

[53] UN Web TV, (2nd meeting) Open-ended working group on security of and in the use of information and communications technologies 2021–2025, Third substantive session, 25 July 2022, https://media.un.org/en/asset/k1a/k1a978izhq (starts at 7:52), and also here: Remarks by the delegation of Brazil on the draft progress report (sections: introduction, threats, norms), 27 July 2022, p. 2, https://documents.unoda.org/wp-content/uploads/2022/07/Brazil-part-1.pdf

[54] UN Web TV, (2nd meeting) Open-ended working group on security of and in the use of information and communications technologies 2021–2025, Third substantive session, 25 July 2022, https://media.un.org/en/asset/k1a/k1a978izhq (starts at 27:10)

[55] UN Web TV, (2nd meeting) Open-ended working group on security of and in the use of information and communications technologies 2021–2025, Third substantive session, 25 July 2022, https://media.un.org/en/asset/k1a/k1a978izhq (starts at 27:45)

Cameroon**: "**We believe it is important to support states in all of their capacity in order to fill gaps as well as to address issues with IP addresses."[56]

The Netherlands: "We welcome the reference to the general availability and integrity of the Internet. As an editorial point I would request for this concept to be reflected in line with the 2021 OEWG and GGE reports. In these reports the concept is referred to as: "the technical infrastructure essential to the general availability or integrity of the Internet."[57]

27 July 2022

Pakistan: "Pakistan highly supported the idea of CBMs and further recommended steps which call for increasing the cooperation among respective CERTS of the member states who address investigation or respect[ive] requests of internet protocols and to resolve technical impediments in the field of cyber attribution."[58]

First Annual Progress Report of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025

The first annual progress report of the OEWG summed up the views, discussions and proposals put forth at the OEWG session in 2021–2022. As such it served as a consensus document to pave the way toward discussions in 2023.[59]

8 August 2022

The OEWG First Annual Progress Report: "Of specific concern is malicious ICT activity affecting critical information infrastructure, infrastructure providing essential services to the public, the technical infrastructure essential to the general availability or integrity of the Internet and health sector entities."

Context: The above wording was taken from the 2021 U.N. Group of Governmental Experts report.[60]

---

[56] UN Web TV, (2nd meeting) Open-ended working group on security of and in the use of information and communications technologies 2021–2025, Third substantive session, 25 July 2022, https://media.un.org/en/asset/k1a/k1a978izhq (starts at 43:42)

[57] UN Web TV, (2nd meeting) Open-ended working group on security of and in the use of information and communications technologies 2021–2025, Third substantive session, 25 July 2022, https://media.un.org/en/asset/k1a/k1a978izhq (starts at 1:31:53)

[58] UN Web TV, (5th meeting) Open-ended working group on security of and in the use of information and communications technologies 2021–2025, Third substantive session, 27 July 2022, https://media.un.org/en/asset/k10/k100qzajqy (starts at 8:35)

[59] Report of the open-ended working group on security of and in the use of information and communications technologies 2021–2025, Open-ended Working Group on security of and in the use of information and communications technologies 2021-2025, Final reports, 22 August 2022, https://meetings.unoda.org/meeting/57871/documents?f%5B0%5D=document_type_meeting%3AFinal%20reports

[60] Report of the 2021 GGE, A/76/135, consensus GA resolution 76/19, 14 July 2021, para 10, https://documents.un.org/prod/ods.nsf/xpSearchResultsM.xsp

The OEWG First Annual Progress Report: “States could strengthen coordination and cooperation between States and interested stakeholders, including businesses, non-governmental organizations and academia. States noted that stakeholders are already playing an important role through partnerships with States for the purposes of training, research, and facilitating access to Internet and digital services.” [61] [62]

Informal Consultations

The OEWG Chair convened several informal consultations in the intersessional period. The quotes below were taken from published materials on the OEWG website.

On 7 December 2022, Russia submitted the following statement to the OEWG informal consultations: “At the current stage of ICT-development trustworthy and unequivocal identification of the source of malicious activity is not possible without fundamentally reforming the protocols of the global communication network and organizing the necessary interstate cooperation. With that in mind, the establishment of clear mechanisms for interaction between competent State agencies becomes especially needed.”[63]

Context: The Russian Federation has provided no evidence that there is a need for “fundamentally reforming the protocols” of the Internet to achieve the described goal. Common Internet protocols such as the Transmission Control Protocol/Internet Protocol (TCP/IP) enable communications between devices. The Internet Engineering Task Force (IETF) is responsible for the TCP/IP suite. Any changes to the TCP/IP suite are managed by the IETF, which is open to anyone to participate.

In the same submission, Russia added: “There are no universally recognized norms in the field of countering the use of ICTs for terrorist and criminal purposes, suppressing the dissemination of illegal content and fakes, and the internationalization of Internet governance.”[64]

---

[61] First Annual Progress Report of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025, 8 August 2022, p. 13, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N22/454/03/PDF/N2245403.pdf?OpenElement

[62] Representatives of the Russian Federation and Ukraine blocked the participation of some non government entities in the work of the OEWG.. A total of 32 organizations were excluded from the proposed accreditation list# of the OEWG sessions because member states had reached consensus on the modalities of participation of non government entities earlier. The consensus specifically indicated that non-ECOSOC-accredited entities will be able to participate in the work of the OEWG on a non-objection basis. Ukraine objected to the participation of five organizations from Russia. Russia objected to the participation of 10 organizations from the USA, four organizations from the United Kingdom, three international organizations, two organizations from Germany, and one organization respectively from Australia, Finland, France, Ireland, Nigeria, Spain, Switzerland, and Uganda.

[63] Statement by the representative of the Russian Federation at the informal intersessional meeting of the Open-Ended Working Group on Security of and in the Use of ICTs 2021-2025 New York, 7 December 2022, p. 1, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Russia_-_statement_on_international_law_-_OEWG_intersessionals_07.12.2022.pdf

[64] Statement by the representative of the Russian Federation at the informal intersessional meeting of the Open-Ended Working Group on Security of and in the Use of ICTs 2021-2025 New York, 7 December 2022, p. 2, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Russia_-_statement_on_international_law_-_OEWG_intersessionals_07.12.2022.pdf

Context: There are universally recognized documents, mentioned already — the WSIS Tunis Agenda and the WSIS+10 Outcome Document — which explain and affirm the multistakeholder model of Internet governance as a result of a truly international effort.

Forth substantive session[65]

On 7 March 2023, Singapore said: "We also recall the proposals in the annex of the Chair's summary on protecting the technical infrastructure essential to the general availability or integrity of the Internet. Such technical infrastructure suggests DNS – the Domain Name System or Internet exchange points are important for developed and developing states alike, given the increased reliance of all states on ICT-based technologies. We support further discussion within the OEWG on possible measures that can be taken to ensure the availability or integrity of the Internet".[66]

Fifth substantive session

On 27 July 2023, Portugal said, among others, talking about the four items that didn't make it in the annual OEWG report: "…3. The reaffirmation that essential services and critical infrastructure should always be off limits for malicious cyber activity, 4. The recognition of the essential roles of all stakeholders, including the tech platform, to every pillar of the framework, namely in … protecting critical infrastructure…"[67]

On 28 July 2023, Russia quoted from the declaration of the Russia - Africa summit on ICTs[68] and made the following statement: "We note the need to bolster the coordination between the Russian Federation and African states in international organizations under the UN system when it comes to postal services, and the ITU. In particular when it comes to developing documents to develop ICTs. We are guided by the fact that the Tunis Program for Information Society should be developed. It was adopted in 2005 at the WSIS forum. We support the creation of a balanced international system to manage the Internet under the auspices of the United Nations so as to avoid any unilateral political limitations or commercial interests and to ensure the safety and stability of the critical information infrastructure of the world web."[69]

Context: There is no evidence that there has been any limitation threatening the "safety and stability of the critical information infrastructure of the world web." Further, there is no evidence that the existing international system to manage the Internet is not balanced, or that it needs to be moved under the auspices of any intergovernmental organization, including the United Nations. In fact the Russian Federation participates in that very system as a member of the ICANN Governmental Advisory Committee.[70]

---

[65] Some of the statements during the fourth substantive session of the OEWG contained quotes that were repetitive and have already been cited in our update report.
[66] UN Web TV, (3rd meeting) Open-Ended Working Group on Information and Communication Technology (ICT) - Fourth Substantive Session,7 March 2023, (starts at 2:11:30), https://media.un.org/en/asset/k1a/k1ah2cv3gr
[67] UN Web TV, (8th meeting) Open-Ended Working Group on Information and Communication Technology (ICT) - Fifth Substantive Session, 27 July 2023, (starts at 2:11:52), https://media.un.org/en/asset/k1n/k1ngmoogyi
[68] Declaration of the Second Russia–Africa Summit on Cooperation in the Field of International Information Security July 28, 2023, paragraph 7, http://en.kremlin.ru/supplement/5975
[69] UN Web TV, (10th meeting) Open-ended working group on Information and Communication Technology (ICT) - Fifth Substantive Session, 28 July 2023, (starts at 11:00), https://media.un.org/en/asset/k1s/k1san5j55u
[70] ICANN | GAC, Governmental Advisory Committee, https://gac.icann.org/

On 28 July 2023, the OEWG adopted the 2nd draft annual progress report.[71] The report contained the following language:

"States also highlighted that malicious ICT activities against CI and CII that undermine trust and confidence in political and electoral processes, public institutions, or that impact the general availability or integrity of the Internet, are also a real and growing concern. States expressed particular concern regarding malicious ICT activities that are aimed at interfering in the internal affairs of States."[72]

"States underlined the importance of the protection of Critical Infrastructure (CI) and Critical Information Infrastructure (CII). States highlighted that ICT activity that intentionally damages CI or CII or otherwise impairs the use and operation of CI or CII to provide services to the public can have cascading domestic, regional and global effects. It poses an elevated risk of harm to the population and can be escalatory. States thus emphasized the need to continue to strengthen measures to protect all CI and CII from ICT threats and proposed increased exchanges on best practices with regard to CI and CII protection, including the sharing of national policies, and recovery from ICT incidents involving CI and CII. In this regard, States recalled General Assembly resolution 58/199 on the "Creation of a global culture of cybersecurity and the protection of critical information infrastructures" and its accompanying annex. States also proposed to support developing countries and small States, in their identification of national CI and CII, where requested."[73]

The annual progress report also contains the following recommendation: "At the sixth, seventh and eighth sessions of the OEWG, States to also undertake focused discussions on: (a) strengthening measures to protect CI and CII from ICT threats, including exchanges on best practices to detect, defend against or respond to, and recover from ICT incidents, and to support developing countries and small States in their identification of national CI and CII, where requested; and (b) further cooperation and assistance to ensure the integrity of the supply chain and prevent the use of harmful hidden functions."[74]

[71] Report of the open-ended working group on security of and in the use of information and communications technologies 2021–2025, Open-ended Working Group on security of and in the use of information and communications technologies 2021-2025, Final reports, August 1, 2023, https://meetings.unoda.org/meeting/57871/documents?f%5B0%5D=document_type_meeting%3AFinal%20reports

[72] Open-ended working group on security of and in the use of information and communications technologies 2021-2025 Fifth substantive session, New York 24-28 July 2023, Second Annual Progress Report, p. 6, https://documents-dds-ny.un.org/doc/UNDOC/LTD/N23/227/59/PDF/N2322759.pdf?OpenElement

[73] Ibid, p. 8

[74] Ibid, p. 9

U.N. Ad-hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (AHC)[75]

First session (submissions related to the first session of the AHC)[76]

29 June 2021

Russian Federation: ""Critical information infrastructure" shall mean an assemblage of critical information infrastructure facilities and telecommunications networks used to interconnect critical information infrastructure facilities; n) "Critical infrastructure facilities" shall mean information systems and information and communications networks of public authorities and information systems and automated process control systems operating in the defense, healthcare, education, transport, communications, energy, banking and finance sectors, nuclear and other important areas of the life of the state and society".[77]

8 November 2021

Interpol: "Access to critical domain name registration information (WHOIS data) is limited for law enforcement in the current regulatory environment. To support law enforcement worldwide in this key challenge, INTERPOL has designed and launched the pilot testing of a new restricted portal, providing automated access to domain registration information to vetted law enforcement entities. Following the successful completion of the pilot phase of the system, INTERPOL is integrating this solution into its global police capabilities with the necessary legal agreements in place to expand the pool of private operators involved and open the system to the member countries".[78]

---

[75] This chapter contains quotes from the 6 sessions of the AHC, and is structured to reflect contributions during First and Second sessions. The quotations from the Third session also include recorded discussions that took place on the floor of the AHC. The Fourth and Fifth sessions resulted in the publication of the draft text, that was titled "a consolidated negotiating document", and the Sixth session produced the "draft text of the convention". This chapter includes relevant quotes from these documents. See here: Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Meetings of the Ad Hoc Committee: Sessions, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

[76] First session of the Ad Hoc Committee, New York, 28 February to 11 March 2022, Submissions from Member States related to the first session of the ad hoc committee, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-first-session.html

[77] United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Draft, Unofficial translation, Submission by Russian Federation related to the first session of the Ad Hoc Committee, 29 June 2021, p.6, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_E.pdf

[78] INTERPOL's contribution to the elaboration of a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Submission by Interpol related to the first session of the Ad Hoc Committee, 8 November 2021, p. 6,

Second session (submissions related to the second session of the AHC)[79]

7 April 2022

Russian Federation (on behalf of Belarus, Burundi, China, Nicaragua, and Tajikistan): "Each State party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: [...] (b) A service provider offering its services in the territory of that State party to submit subscriber information in that service provider's possession or control." [...] "For the purposes of this article, the term "subscriber information" shall mean any information held by a service provider relating to subscribers to its services other than traffic data or content data, on the basis of which it is possible to establish: "b) The subscriber's identity, postal or other addresses, telephone and other access numbers, including IP addresses and billing and payment information, available in the service agreement or arrangement; (c) Information relating to the location of information and telecommunications equipment that has a bearing on the service agreement or arrangement."[80]

8 April 2022

Brazil: "(i) 'Subscriber data' means any computer data, collected in the normal course of business by a service provider, pertaining to the name, date of birth, postal or geographic address, billing and payment data, device identifiers, telephone number, or email address, or any other information, such as the IP address used at the time when an account was created, which can serve to identify the subscriber or customer, as well as the type of service provided and the duration of the contract with the service provider, other than traffic or content data."[81]

Islamic Republic of Iran: "the convention should specify and stipulate obligations and regulations as to the cooperation of the private sector, service providers and other similar entities with law enforcement, in particular sectors and providers with global or substantial outreach at the international level."[82]

Japan: "Cybersecurity and Internet governance should not be addressed in this convention. For example, the following measures would have a chilling effect on legitimate economic activity

https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/IGOs/21COM1175-SRIUN_UseInformation_CriminalPurposes_complet.pdf

[79] Second session of the Ad Hoc Committee, Vienna, 30 May to 10 June 2022, Submissions related to the second session of the Ad Hoc Committee, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-second-session.html

[80] Submission by Russian Federation also on behalf of Belarus, Burundi, China, Nicaragua, and Tajikistan related to the second session of the Ad Hoc Committee, 7 April 2022, p. 13, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Russia_Contribution_E.pdf

[81] Brazil's proposal on initial chapters of a United Nations convention on cybercrimes, Submission by Brazil related to the second session of the Ad Hoc Committee, 8 April 2022, p. 2, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Brazil_Contribution_E.pdf

[82] Submission by Islamic Republic of Iran related to the second session of the Ad Hoc Committee, 8 April 2022, p. 4, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Islamic_Republic_of_Iran_contribution.pdf

and would impede the development of technology, and would go beyond the mandate of the Ad Hoc Committee:

- setting security standards under this convention;
- imposing obligations on legal persons and individuals to comply with such standards or imposing penalties for violation of such standards; or
- holding legal persons, their representatives, or software creators who unintentionally engaged in cybercrimes committed by other actors without awareness, accountable."[83]

9 April 2022

Canada: Suggested defining "computer data" as "any representation of facts, information, or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function. This definition would include all types of data: content data (the actual message), computer programs, traffic data, subscriber information, passwords, and connection codes. According to the same contribution, "traffic data" shall mean "any computer data to identify, activate or configure a device relating the creation, transmission or reception of a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination or termination, route, time, date, size, duration, or type of underlying service. This definition includes, for both telephony and internet services, the data necessary for dialing, routing and addressing or signaling, for example: phone numbers, date and time of a call (and other elements in call data logs), the source and destination of messages (such as communication's origin, destination or termination, route, time, date, size, duration, or type of underlying service. email or text messages), as well as IP addresses and data pertaining to the protocol used."[84]

12 April 2022

Vietnam: Suggested defining Cyberspace as "a network of information technology (IT) infrastructure which includes telecommunications networks, the Internet, computer networks, communication systems, information processing and control systems, databases."[85]

13 April 2022

Mexico: "Mexico considers that other general provisions must be added on the following issues: [...] the recognition of the public core of the Internet and the relevance of the net neutrality approach for the purposes of the convention."[86]

14 April 2022:

[83] Japan, Contribution on Criminalization, General Provisions, and Procedural Measures and Law Enforcement, Submission by Japan related to the second session of the Ad Hoc Committee, 8 April 2022, pp. 5 - 6, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Japan_Contribution.pdf

[84] Canada, Submission of draft text and contributions on the specific chapters and provisions to be examined during the second session of the Ad Hoc Committee, namely on criminalization, general provisions and procedural measures and law enforcement, 9 April 2022, p.1, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Canada_Contribution.pdf

[85] Submission of Vietnam for the Second Session of the Ad Hoc Committee, 12 April 2022, p. 1, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Vietnam_Contribution.pdf

[86] Contribution of the Government of Mexico for consideration by the Ad Hoc Committee at its second substantive session, 13 April 2022, p. 3, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Mexico_Contribution.pdf

South Africa: "Each State Party shall maintain a register with identifiable information of all Domain name registrars, Crypto Asset Traders and Crypto Assets within its jurisdiction, in accordance with fundamental principles of its domestic law, and supply such information to competent authorities for investigative and evidentiary purpose."[87]

Third session (submissions related to the Third Session of the AHC)[88]

29 August 2022

Islamic Republic of Iran: "Private entities, such as service providers, including in the field of domain names, have a particularly important role in fighting crimes committed via ICT. Given the rampant criminal misuse of services provided, cooperation of such entities with law enforcement and their due diligence in this area, especially the entities with substantial outreach and activities at international level, remains vital. In this respect the Convention should set out regulations and obligations on effective cooperation of these entities with law enforcement. Also such entities should respect the economic, social, legal and cultural specificities of states."[89]

China: "The states shall not in violation of the laws of the state where the data is stored directly collect the data stored in foreign states, from enterprises or individuals or by technical means by passing network security protection measures."[90]

Canada: "Although Canada is not opposed to the inclusion article 32 of the Budapest Convention we are of the view that it might be unwieldy to find the consensus on such an article given the tight timelines under which we are operating for this Convention and given that that article was the result of lengthy discussions."[91]

Context: Article 32, on trans-border access to stored computer data with consent or where publicly available, of the Budapest Convention on Cybercrime reads as follows:

"A Party may, without the authorization of another Party:

a. access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

[87] South Africa's contribution on the provisions on criminalisation, the general provisions and the provisions on procedural measures and law enforcement, 14 April 2022, p. 13, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/South_Africas_contribution.pdf
[88] Third session of the Ad Hoc Committee 29 August to 9 September 2022, New York, Submissions related to the third session of the Ad Hoc Committee, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_third_session/main.html
[89] UN Web TV, (1st meeting) Third Session, Ad Hoc Committee for countering the use of ICT for criminal purposes, 29 August 2022, (starts at 1:08:56), https://media.un.org/en/asset/k1x/k1xh926qrt
[90] UN Web TV, (1st meeting) Third Session, Ad Hoc Committee for countering the use of ICT for criminal purposes, 29 August 2022, (starts at 2:13:22), https://media.un.org/en/asset/k1x/k1xh926qrt
[91] UN Web TV, (2nd meeting) Third Session, Ad Hoc Committee for countering the use of ICT for criminal purposes, 29 August 2022, (starts at 1:43:42), https://media.un.org/en/asset/k1j/k1jbh2v1z7

access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.."[92]

Chile: "But in addition to evidence, one needs essential evidence for any crime and that includes the Internet, or any other procedure connected to the net, or which may be used to support the crime or not."[93]

1 September 2022

Ecuador: "Ecuador in this regard has identified several needs. They would be too many to quote them all of at this time, but by way of example I can mention the current problems with ISPs – the Internet service providers since they don't want to have IPv4 adresses and they have had to use protocols such as the CGNET which makes it possible for thousands of users to use the same IP public address. This makes it difficult to identify who committed the cybercrime. And in this regard we ask that the future Convention include a provision requiring state parties to organize their internal norms in order to ask ISPs that within a reasonable period of time they totally migrate out of IPv4 to IPv6. This would make it possible to have favorable results in investigating cybercrimes and therefore it would be possible to meet the requirements of technical assistance in this field."[94]

The Chair commented on this issue: "We see with you that there are various differences with IP addresses and this is – gives us a lot of room for progress, and this allows us to see that at the levels of technical understanding there are tremendous differences."[95]

Oman: "I associate myself with the statement delivered by the representative of Ecuador vis-a-vis the importance of exchanging working mechanisms and moving from the 4th protocol to the 6th protocol. This would have a positive impact [...] in tackling cybercrime. When companies or service providers, when they change the protocol they work on, I refer to the 6th protocol, this would have a far greater impact in terms of countering cybercrime."[96]

7 September 2022

Pakistan: "Pakistan has always supported the idea of CBMs and further proposes the following recommended action which calls for increasing cooperation among the respective Computer Emergency Response Teams (CERTs) of the Member States to address investigation / trace-

[92] Council of Europe, European Treaties Series - No. 185, Convention on Cybercrime, Budapest, 23 November 2001, p. 17, https://rm.coe.int/1680081561
[93] UN Web TV, (2nd meeting) Third Session, Ad Hoc Committee for countering the use of ICT for criminal purposes, 29 August 2022, (starts at 2:37:05), https://media.un.org/en/asset/k1j/k1jbh2v1z7
[94] UN Web TV, (8th meeting) Third Session, Ad Hoc Committee for countering the use of ICT for criminal purposes, 1 September 2022, (starts at 1:54:12), https://media.un.org/en/asset/k1o/k1o39wyquf
[95] UN Web TV, (8th meeting) Third Session, Ad Hoc Committee for countering the use of ICT for criminal purposes, 1 September 2022, (starts at 1:58:09), https://media.un.org/en/asset/k1o/k1o39wyquf
[96] UN Web TV, (8th meeting) Third Session, Ad Hoc Committee for countering the use of ICT for criminal purposes, 1 September 2022, (starts at 02:06:20), https://media.un.org/en/asset/k1o/k1o39wyquf

back requests of Internet Protocols and to resolve the technical impediments in the way of cyber attribution."[97]

Russia: "Russian Federation suggested the addition of the following paras to the document (report): [...] States note the importance of adopting measures to safeguard the general availability, secure and stable functioning of the Internet taking into account States' sovereignty in their information space, as well as to ensure equal participation of States in the governance of this network."[98]

Context: As in the interventions at the OEWG, Russia does not provide evidence that there is unequal participation of States in the governance of the Internet. As explained above, the Russian Federation is a member of the ICANN GAC, and as such, participates on equal footing with all other GAC members in the work of ICANN.

Fourth[99] and Fifth sessions[100] of the AHC.

Consolidated AHC negotiating document:

Consolidated negotiating document with the status "as of 21 April 2023" was published after the Fifth sessions of the AHC. The negotiating document contained the draft text of the U.N. cybercrime convention prepared by the Chair of the Ad-hoc Committee. Not all suggestions were accepted by the delegations and more additions were made to the text of the draft convention. However we are quoting the text here as it has relevance.

21 April 2023

Consolidated negotiating document:

India, Pakistan, US, China, New Zealand, Egypt, Kenya, Sudan, Australia, Russia, Colombia, Norway, Canada, Tanzania, Syrian Arab Republic, Algeria, Burkina Faso, Singapore, South Africa, Nicaragua, Macao, Tonga, European Union and member states, and Fiji declared that they want to delete draft article 72 on "cross-border access to stored [computer data] [electronic/digital information] with consent or where publicly available" from the Consolidated negotiating document on the preamble, the provisions on international cooperation, preventive measures, technical assistance and the mechanism of implementation, and the final provisions of a comprehensive international convention on countering the use of information and

[97] Compendium of statements in explanation of position on the adoption of the progress report of the open-ended working group as contained in A/77/275, annex, 7 September 2022, p. 26, https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/oewg-II/documents/compendium_2022.pdf

[98] Compendium of statements in explanation of position on the adoption of the progress report of the open-ended working group as contained in A/77/275, annex, 7 September 2022, p. 37, https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/oewg-II/documents/compendium_2022.pdf

[99] This Chapter does not contain any quotations from the Fourth session of the Ad Hoc Committee. For your reference please see the Fourth session of the Ad Hoc Committee, 9 - 20 January 2023, Vienna, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_fourth_session/main.html

[100] Fifth session of the Ad Hoc Committee, 11-21 April 2023, Vienna, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_fifth_session/main

communications technologies for criminal purposes. Two countries – Ecuador and Venezuela – were for retaining the text of this article after the edits.[101] The full text of the article reads:

"A State Party may, without the authorization of another State Party:
(a) Access publicly available (open source) stored [computer data] [electronic/digital information], regardless of where the [data are] [information is] located geographically; or
(b) Access or receive, through [a computer system] [an information and communications technology system/device] in its territory, stored [computer data] [electronic/digital information] located in another State Party, if the State Party accessing or receiving the [data] [information] obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the [data] [information] to that State Party through that computer system."[102]

Malaysia, Angola, and Namibia chose to exclude only part "b)" of the draft article.

Comment: The follow-up advance copy of the draft text of the convention prepared for the 6th session of the AHC, did not contain draft article "Article 72 on cross-border access to stored [computer data] [electronic/digital information] with consent or where publicly available" analogous to article 32 of the Budapest Cybercrime Convention.[103]

Sixth session of the AHC.[104]

The work of the Sixth session of the AHC concluded on 1 September, 2023.

Draft text of the convention (version as of 2 September 2023)

The Sixth session of the AHC produced the 80-page long text of the draft convention on cybercrime. We would like to draw your attention to the following provisions of this text and comment on some of them.

"Article 2. Use of terms.

[...]

(c) "Traffic data" shall mean any [computer data] [digital information] collected by a service provider, excluding content data, related to: (i) The type of service provided and its duration

[101] Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Fifth session 11 - 21 April 2023, Consolidated negotiating document on the preamble, the provisions on international cooperation, preventive measures, technical assistance and the mechanism of implementation and the final provisions of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes, p. 38, 21 April 2023, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/5th_session/Documents/CND_2_-_21.04.2023.pdf
[102] Ibid
[103] Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Sixth session, 21 August - 1 September, 2023, Draft Convention (advance copy), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Pre-session-docs/A_AC_291_22_Advance_Copy.pdf
[104] Sixth session of the Ad Hoc Committee, 21 August - 1 September 2023, New York, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_sixth_session/main

where it concerns technical data and data identifying related technical measures or interfaces used by or provided to the subscriber or customer, and data related to the validation of the use of the service, excluding passwords or other authentication means used instead of a password, that are provided by a user or created at the request of a user; (ii) The commencement and termination of a user access session to a service, such as the date and time of use, or of the login to and logout from the service; and (iii) Communications metadata processed in an electronic communications network for the purposes of transmitting, distributing or exchanging content data, including data used to trace and identify the source and destination of a communication, data on the location of the terminal equipment used in the context of providing communications services, and the date, time, duration and type of the communication;"[105]

Comment: This differs from the definition provided in the Budapest Convention on Cybercrime. According to the Budapest Convention: "'traffic data means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service."[106]

The Budapest Convention on Cybercrime provides the same definitions of "service provider" and "subscriber information"[107] but does not provide the definition of "content data." It is provided by the draft U.N. Convention.[108]

[...]

The Dominican Republic added the draft provision to "Article 2. Use of terms." It wants to define who the "relevant stakeholders"[109] are.

Russian Federation, Iran, Belarus, Burkina Faso, Venezuela, Egypt introduced: "Article 10 bis. Unlawful interference with critical information infrastructure.
1. Each State party shall adopt such legislative and other measures as are necessary to establish as an offence under its domestic law the intentional creation, distribution and/or use of software or other digital information knowingly designed to interfere unlawfully with critical information infrastructure, including software or other digital information for the destruction, blocking, modification, copying of information contained therein, or for the neutralization of

[105] Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Sixth session, 21 August - 1 September, 2023, Draft text of the convention (Status as of 2 September 2023 with updates from Member States), p.3, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/DTC/DTC_rolling_text_02.09.2023.pdf

[106] Council of Europe, Convention on Cybercrime, Budapest, 23 November, p. 3, https://rm.coe.int/1680081561

[107] Council of Europe, European Treaty Series - No. 185, Convention on Cybercrime, Budapest, 23 November 2001, pp. 3 and 9, https://rm.coe.int/1680081561

[108] "(d) "Content data" shall mean any [computer data] [digital information] relating to a communication by means of a [computer system] [information and communications technology device] concerning the substance or purport of that communication, such as text, voice messages, audio recordings, video recordings and other types of information." The European Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data provides the definition of "personal data" – a term that has a similar formulation in the text of the draft U.N. convention: "Personal data" shall mean data relating to an identified or identifiable natural person." Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Sixth session, 21 August - 1 September, 2023, Draft text of the convention (Status as of 2 September 2023 with updates from Member States), pp.3 - 4, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/DTC/DTC_rolling_text_02.09.2023.pdf

[109] Ibid, p. 4

security features. 2. Each State party shall adopt such legislative and other measures as are necessary to establish as an offence under its domestic law the violation of the rules of operation of media designed for storage, processing and transfer of protected digital information contained in critical information infrastructure or information systems or information and communication networks that belong to critical information infrastructure, or the violation of the rules of access to them, if such violation damages the critical information infrastructure. "[110]

Comment: Australia, United States, EU & its member states, New Zealand, Georgia, Norway, United Kingdom, Liechtenstein, Canada, Chile, Japan, Mexico are against the inclusion of this article into the convention and are asking to delete it.

China, Iran, Russian Federation, Venezuela, Iran, Egypt introduced:
"Article 10 ter. Unlawful provision of service.
Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right
(a) The provision of service or technical support, including internet access, server hosting, online storage, communications transmission or similar services; or
(b) The creation of websites, communication networks

with the intent that the service or technical support be used for the commission of any of the offences established in accordance with this Convention."[111]

Comment: Australia, United States, EU & its member states, New Zealand, Georgia, Norway, United Kingdom, Liechtenstein, Canada, Japan, Mexico are against the inclusion of this article into the convention and are asking to delete it.

Russian Federation, Mali, Belarus, Nicaragua, Burkina Faso, Eritrea, Venezuela, Sudan, Cuba, Nigeria, Burundi, DPRK, Egypt, Turkey, Sierra Leone submitted: "Article 15 septies. Terrorism-related offences.
Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed by means of information and communications technologies, the commission of terrorist acts, the incitement, recruitment or other involvement in terrorist activities, the advocacy and justification of terrorism or the collection or provision of funds for its financing, training for terrorist acts, the facilitation of communication between terrorist organizations and their members, including the establishment, publication or use of a website or the provision of logistical support for perpetrators of terrorist acts, the dissemination of methods for making explosives employed in particular in terrorist acts, and the spreading of strife, sedition, hatred or racism."[112]

Comment: Canada, United States, New Zealand, Dominican Republic, Guatemala, Norway, Georgia, Australia, EU & its member states, Israel, United Kingdom, Lebanon, Liechtenstein, Chile, Japan, Mexico are against the inclusion of this article into the convention and are asking to delete it.

Algeria, Canada, Russian Federation proposed to retain the original text of:

[110] Ibid, p. 9
[111] Ibid, p. 9
[112] Ibid, p.19

Article 21. Prosecution, adjudication and sanctions
[...]
"Each State Party may adopt, in accordance with its domestic law, such legislative and other measures as may be necessary to establish aggravating circumstances in relation to the offences established in accordance with articles 6 to 9 of this Convention, including circumstances that affect critical information infrastructures."[113]

Comment: Liechtenstein, New Zealand, Norway, Tanzania, United States, EU and its member states, Switzerland, Nigeria, Israel, Philippines, Australia, Georgia, Norway, CARICOM are against the inclusion of this article into the convention and are asking to delete it.

"Article 26. Expedited preservation and partial disclosure of traffic data
Each State Party shall adopt, in respect of traffic data that are to be preserved under the provisions of the article on the expedited preservation of stored [computer data] [digital information], such legislative and other measures as may be necessary to: [...] (b) Ensure the expeditious disclosure to the State Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the State Party to identify the service providers and the path through which the communication or indicated information was transmitted."[114]

"Article 27. Production order
Each State Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: [...] (b) A service provider offering its services in the territory of the State Party to submit subscriber information relating to such services in that service provider's possession or control."[115]

The Russian Federation, Argentina, Venezuela, Egypt, South Africa were in favor of retaining the text of the following article:
"Article 29. Real-time collection of traffic data[116] 1. Each State Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: (a) Collect or record, through the application of technical means in the territory of that State Party; and (b) Compel a service provider, within its existing technical capability: (i) To collect or record, through the application of technical means in the territory of that State Party; or (ii) To cooperate and assist the competent authorities in the collection or recording of; traffic data, in real time, associated with specified communications in its territory transmitted by means of [a computer system] [an information and communications technology device]. 2. Where a State Party, owing to the principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1 (a), it may instead adopt legislative and other measures as may be necessary to

[113] Ibid, p. 25

[114] Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Sixth session, 21 August - 1 September, 2023, Draft Convention (advance copy), page 13, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Pre-session-docs/A_AC_291_22_Advance_Copy.pdf

[115] Ibid

[116] On September 1, 2023 Chair of the AHC Group, discussed Articles 29 and 30 (Real Time Collection of Traffic Data and Interception of Content Data respectively) and said: "However regarding articles 29 and 30 several delegations requested reservations to facilitators to propose amendments and they expect further discussions at the 7th session of the Committee." UN Web TV, (23rd meeting) Sixth session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, 1 September 2023, (starts at 02:01:23), https://media.un.org/en/asset/k17/k17lzfhyyp

ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means in that territory. 3. Each State Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it."[117]

Comment: Singapore, Switzerland, Malaysia, Vietnam are against the inclusion of this article into the convention and are asking to delete it.

"Article 36. Protection of personal data.
1. A State Party transferring personal data pursuant to this Convention shall do so subject to the conditions of that State Party's domestic law and applicable international law. States Parties shall not be required to transfer personal data in accordance with this Convention if it cannot be provided in compliance with their applicable laws concerning the protection of personal data. They may also seek to impose conditions, in accordance with such applicable laws, to achieve compliance in order to respond to a request for personal data. States Parties are encouraged to establish bilateral or multilateral arrangements to facilitate the transfer of personal data."[118]

CARICOM, EU & its member states, Vanuatu, New Zealand, Albania, Georgia, United States, United Kingdom, China, Norway, Cabo Verde, Tanzania, Lebanon, Colombia, Ecuador, Pakistan, Switzerland, Tonga, Australia supported the inclusion of this provision into Article 36: "1 bis. Where the transfer of personal data cannot be carried out in accordance with paragraph 1, States Parties may seek to impose appropriate conditions (in compliance with their applicable laws concerning the protection of personal data [...] to achieve compliance in order to respond positively to a request for personal data."[119]

Comment: India proposed to delete the above additional provision.

Russian Federation proposed this addition in:
"Article 40. General Principles and procedures relating to mutual legal assistance. [...] 3. Mutual legal assistance to be afforded in accordance with this article may be requested for any of the following purposes: [...] [(l bis) Removal of the domain name used for criminal activities."[120]

"Article 43. Expedited disclosure of preserved traffic data
1. Where, in the course of the execution of a request made pursuant to article 42 to preserve traffic data concerning a specific communication, the requested State Party discovers that a service provider in another State Party was involved in the transmission of the communication, the requested State Party shall expeditiously disclose to the requesting State Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted."[121]

Article 45. Mutual legal assistance in the real-time collection of traffic data

[117] Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Sixth session, 21 August - 1 September, 2023, Draft text of the convention (Status as of 2 September 2023 with updates from Member States), p. 33 https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/DTC/DTC_rolling_text_02.09.2023.pdf
[118] Ibid, p. 38
[119] Ibidem
[120] Ibid, p. 47
[121] The state parties agreed "ad referendum" to this provision, Ibid, p. 26

1. States Parties shall provide mutual legal assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of [a computer system] [an information and communications technology device]. Subject to the provisions of paragraph 2, such assistance shall be governed by the conditions and procedures provided for under domestic law."

[...]

"3. A request made in accordance with paragraph 1 of this article shall specify: (c) The [computer data] [digital information] in relation to which the collection of the traffic data is required and their relationship to the offense or other illegal act; (d) Any available data that identify the owner or user of the data or the location of the [computer system] [information and communications technology device];"[122]

Context: The AHC was having the informal consultations in the inter-sessional period between the 6th and the last session in January - February 2024. The multi-stakeholders were not invited to these consultations and they are for governments only. The objective of the Chair was to produce a reduced "clean" draft text of the Convention by the end of November 2023.

[122] Ibidem

Global Digital Compact and the Summit of the Future

Introduction/Background

In 2020, Secretary-General Guterres' report, Our Common Agenda, proposed a Summit of the Future, with a technology track leading to a Global Digital Compact (GDC): "Furthermore, building on the recommendations of the road map for digital cooperation (see A/74/821), the United Nations, Governments, the private sector and civil society could come together as a multi-stakeholder digital technology track in preparation for a Summit of the Future to agree on a Global Digital Compact. This would outline shared principles for an open, free and secure digital future for all."[123]

The Global Digital Compact

On 25 April 2023, the U.N. Secretary-General published Policy Brief # 5, which specifically contained language from the U.N secretary-general on the parameters of the framework for the future GDC. Please refer to the ICANN blog where some quotes from the GDC are put into context.[124]

Excerpts from written submissions to the GDC by Member States, Coalitions and Supranational Organizations

Context: The office of the U.N. Envoy on Technology organized a series of deep dives on issues related to the GDC in spring and summer of 2023. ICANN's GE staff was present during these presentations however, the deliberations were not officially recorded and GE cannot provide quotes from these discussions. However, some of the written contributions reflect the oral interventions of country delegations during these deliberations.

April 2023

On 13 April 2023, the European Union stated: "The EU believes that, […] the internet must remain open, global, free, interoperable and decentralized. We strongly support the multistakeholder approach to internet governance, which ensures that all actors, including governments, the private sector, civil society, and technical communities, are involved in shaping the future of the internet."
[…]
"A positive example of furthering the multistakeholder approach was the successful IANA stewardship transition to ICANN in 2016. All stakeholders, including governments, are welcome

[123] Declaration on the commemoration of the seventy-fifth anniversary of the United Nations, Resolution adopted by the General Assembly on 21 September 2020, A/RES/75/1, 28 September 2020, https://documents.un.org/prod/ods.nsf/xpSearchResultsE.xsp
[124] ICANN blogs, 13 June 2023, https://www.icann.org/en/blogs/details/un-secretary-general-policy-report-considerations-for-the-icann-community-13-06-2023-en

to participate in ICANN and can help increase the security and stability of the global domain name system DNS."[125]

The Islamic Republic of Iran stated : "Preparing an effective cooperation framework among the custodians of the internet governance ecosystem as well as the guardians of the IP and management system with law enforcement and judicial authorities of the countries in the prevention and fight against cybercrimes."[126]

The Netherlands stated: "The Global Digital Compact should commit to avoiding a fragmentation of the technical infrastructure of the Internet, impeding the ability of systems to interoperate, and threatening the general integrity and availability of the core Internet infrastructure. This includes packet routing and forwarding, naming and numbering systems, encryption [technologies], and the underlying physical infrastructures."[127]

The G77 and China stated: "The Global Digital Compact should build upon key documents and forums to advance digital cooperation, inter alia, the World Summit on the Information Society (WSIS), in particular the Tunis Agenda and the Geneva Plan of Action, the Internet Governance Forum, and take into account the Secretary-General Roadmap for Digital Cooperation."
[…]
"The Group underscores that the outcomes of the WSIS should be preserved as a guide for digital international cooperation and for Internet governance, since it is based on principles that favor development."
"The Tunis Agenda and the Geneva Declaration of Principles and plan of action shall lay down the guiding principles for the development of any new mechanism on digital cooperation, including GDC."

[...]
"We recognize that no single country or stakeholder, or a small group thereof, should be allowed to monopolize or control the Internet core infrastructure."
"States which have monopoly and dominance in ICT environment, including internet, shall not use ICT advances as tools for containment and suppression of the legitimate economic and technological development of other States."
"The Global Digital Compact should reiterate that the Internet should be open, secure, inclusive, accessible and interoperable."
[...]
"Internet governance should be addressed in a global setup, backed by the UN system, through extensive participation of all States with a multi-stakeholder approach as set out in the WSIS outcomes."
[…]

[125] Delegation of the European Union to the United Nations in New York, EU Statement -- Global Digital Compact: Deep Dive on Internet Governance, 13 April, 2023, https://www.eeas.europa.eu/delegations/un-new-york/eu-statement-global-digital-compact-deep-dive-internet-governance_en?s=63
[126] Contribution of the Islamic Republic of Iran to the Global Digital Compact, April 2023, last modified on 2 May 2023, p. 20, https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/GDC-submission_Islamic-Republic-Iran.pdf
[127] Global Digital Compact Submission by the Kingdom of the Netherlands, 28 April 2023, p. 7, https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/GDC-submission-Kingdom-of-the-Netherlands.pdf

"Security, safety and stability of Internet must be maintained, without jeopardizing efforts to achieve sustainable development. International cooperation through strengthening multilateralism in this area is highly important."[128]

El Salvador reaffirmed "… the importance of continuing the multi-stakeholder approach outlined in the Geneva Summit of 2003 and the Tunis Agenda of 2005."[129]

France wrote: **"**Proposed actions: […] Work will also need to be done on protocols to maintain the unity, neutrality and resilience of the Internet."[130]

The People's Republic of China stated: "States have the right to participate in the management and distribution of basic international Internet resources on equal footings, and should refrain from taking advantage of Internet resources and technologies to undermine the legitimate rights of other States to access the Internet, thus endangering the security, stability and connectivity of the global Internet."[131]
[...]
"States should foster a cyberspace featuring peace, security, openness, cooperation and order, and stand against division and fragmentation of the Internet. States should formulate globally interoperable common rules and standards in cyberspace through broad participation of Member States under the auspices of the UN, and stay committed to building an international Internet governance system featuring multilateralism, democracy and transparency."[132]

Informal meeting launching Our Common Agenda Policy Brief #5 A Global Digital Compact — an Open, Free and Secure Digital Future for All[133]

At an informal meeting at U.N. headquarters on 5 June 2023, Secretary-General António Guterres launched Policy Brief # 5. In his introductory remarks, Mr. Guterres said, "The brief proposes a Digital Cooperation Forum that would evaluate progress on digital governance and highlight gaps. This would be the first global framework to bring all stakeholders together to drive aligned action on digital technology. It would work with regional bodies and multistakeholder networks and would support exchanges between existing bodies such as the Internet Governance Forum. It would have wide participation, engage those who develop digital technologies to understand potential and promote their responsible application."[134]

---

[128] G77 and China inputs to the Global Digital Compact discussions, 28 April 2023, https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/GDC-submission_G77-and-China.pdf
[129] National Submission of El Salvador on the Global Digital Compact proposed thematic areas, last modified 1 May 2023, p.3, https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/GDC-submission_El-Salvador.pdf
[130] Global Digital Compact Contribution of France – Courtesy translation, last modified 8 May 2023, p. 5, https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/GDC-submission_France.pdf
[131] China's Positions on Global Digital Governance (Contribution for the Global Digital Compact), last modified 24 May 2023, p.5, https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/GDC-submission_China.pdf
[132] Ibid, p. 13
[133] Please look at the ICANN Blogs page for detailed information regarding the Policy Brief: https://www.icann.org/en/blogs/details/un-secretary-general-policy-report-considerations-for-the-icann-community-13-06-2023-en
[134] Launch of the SG's Our Common Agenda Policy Briefs Briefing by the Secretary-General, Our Common Agenda policy briefs for the Summit of the Future (organized by the Executive Office of the Secretary-General (EOSG), UN Web TV, 7 May 2023, (starts at 19:35),

Responses by delegates of some U.N. Member States:

The European Union (on behalf of its 27 states): “Supporting and strengthening established structures such as the Internet Governance Forum, ITU, UNESCO and others could help avoid duplication and fragmentation of efforts.” […] “A multistakeholder approach would be key in supporting the GDC”[135]

Canada (also on behalf of Australia and New Zealand, or CANZ): “Our countries are fully committed to working with others to ensure the continuation of a free, open, interoperable, relievable and secure Internet globally.” […] We are also strong supporters of the multistakeholder model of Internet governance, which is the foundation of the Internet’s openness, resilience, and stability. A multistakeholder approach recognizes that everyone has a stake at how the Internet is managed. We must acknowledge the role that the existing multistakeholder organizations are successfully playing in the development and operation of the Internet. While we admire the ambition of the proposals in the policy brief, we strongly urge that any potential new initiatives must first aim to strengthen and complement existing successful efforts in global digital cooperation at the U.N.”[136]

Lithuania: “I would especially like to underline the importance of engaging the specialized agencies such as the ITU by giving them a more clearly determined role for contributing to the Compact objectives.”[137]

Pakistan: “We would want to see more on the need to have an intergovernmental process that would direct the compact towards a more developmental direction rather than a regulatory direction and this should be in accordance with the Tunis agenda where the Internet related public policies are the remit, er, sovereign right of the states. We are of course also considering this Digital Cooperation Forum which we would like to see, how it would synergize with the Internet Governance Forum and with the WSIS Forum as well as the Open-ended Working Group on Security in use of ICTs.”[138]

United States of America: “On the Global Digital Compact to ensure transparency, inclusivity and the active and meaningful participation of all stakeholders in the GDC process we encourage the UN to provide opportunities for the stakeholder community to also offer feedback on the GDC policy brief.”[139] “Attempts to direct digital cooperation from New York do not reflect the fact that multistakeholder, multi-sectoral and decentralized approaches offer a more effective means to leverage digital technologies to help achieve the SDGs.”[140]

Switzerland: “The proposal to create a new Digital Cooperation Forum risk to unnecessarily burden the implementation of the Compact. Instead of bringing real added value it threatens to duplicate the efforts already undertaken in the digital structures for existing cooperation. In

---

https://media.un.org/en/asset/k1n/k1nugz7a7n.

[135] Ibidem, (starts at 20:30)

[136] Ibidem, (starts at 30:33)

[137] Ibidem, (starts at 34:00)

[138] Ibidem, (starts at 39:38)

[139] Ibidem, (starts at 1:06:50)

[140] Ibidem, (starts at 1:08:15)

particular, the Internet Governance Forum has demonstrated its effectiveness in the multistakeholder follow-up in the issues covered by the Compact."[141]

Estonia: "To reach universal and meaningful connectivity we need a multistakeholder cooperation that relies on our common values and common principles, as we already agreed in the Tunis agenda."[142]

China: "On the GDC. China supports the United Nations in playing a pivotal role in coordinating the joint efforts of various stakeholders to strengthen digital cooperation, narrow the digital divide and improve the digital governance, so that digital technology can benefit the entire humanity. The process of drafting should be issue-oriented…"[143]

Indonesia: "On the GDC, we take note that the GDC shares similar ideas with the theme of the 2023 Internet Governance Forum. And in this regard we would like to further hear views on how to ensure GDC, in particular the Global Digital Cooperation Forum initiative, would complement the existing process, avoid duplication and strengthen the IGF?"[144]

United Kingdom: "Any new initiative should complement the existing digital cooperation efforts already taking place at the UN. The UK recognizes existing multistakeholder organizations are the building blocks of the open, resilient, and stable Internet."[145]

India: "Our approach should be informed by avoiding duplication of efforts or establishing of parallel processes."[146]

During his closing remarks, the U.N. Secretary General said: "But we need to distinguish what is the scope of the intergovernmental process, as it relates to the sovereignty of the member states, and what is the scope, the areas in which it is better to keep everybody involved to try to make things move in the positive direction. […] I was expecting the question about the Forum[147] because we also have a discussion in our teams. Again, this is not a matter of faith. This is something that we propose, if member states agree – fine, if member states do not agree – nobody would die. But having said so, I think that the question is not a question of duplication. It's a question of where things come together. Because we have several things around. We have the Internet Governance Forum, we have the ITU mechanisms, we have UNESCO mechanisms, but they are separate. And what I believe we need here in New York, close to the General Assembly, something in which these things can be brought together. […] It's not a logic to duplicate, it's a logic to guarantee that there is someplace where all these things are seen together. And this is the only reason why this proposal was put on the table."[148]

---

[141] Ibidem, (starts at 1:10:17)
[142] Ibidem, (starts at 1:12:46)
[143] Ibidem, (starts at 1:18:24)
[144] Ibidem, (starts at 1:19:40)
[145] Ibidem, (starts at 1:24:30)
[146] Ibidem, (starts at 1:34:32)
[147] herein – Digital Cooperation Forum
[148] Launch of the SG's Our Common Agenda Policy Briefs Briefing by the Secretary-General, Our Common Agenda policy briefs for the Summit of the Future (organized by the Executive Office of the Secretary-General (EOSG), UN Web TV, 7 May 2023, (starts at 1:55:11), https://media.un.org/en/asset/k1n/k1nugz7a7n,

Preparatory ministerial meeting of the Summit of the Future - General Assembly, 78th session

On 21 September 2023 a number of ministerial and high-level statements were made on the Global Digital Compact and Internet Governance, including

Rwanda: “Global digital cooperation will be key under GDC [, it] provides such framework of digital cooperation.”[149]

Norway: “We must also work together towards a just global digital transformation and the Global Digital Compact.”[150]

Russia: “We support the inclusion of the questions of technology and innovations into the Summit’s agenda, to overcome the digital inequality and democratization of Internet Governance and regulation of AI with a strict observance of the national sovereignty of all states.”[151]

Bulgaria: “Preservation of the multistakeholder approach and the integrity of the Internet is where we must attain best results.”[152]

Mexico: “We are fully committed to the Global Digital Compact.”[153]

ITU: “These challenges require all stakeholders to work together. The World Summit on the Information Society, and its follow-up process, like the IGF and WSIS Forum, have an important role to play and that has been recognized by the co-facilitators of the Global Digital Compact.”[154]

India: “We welcome the SoTF aim to deliver the Global Digital Compact, to minimize any digital divide.”[155]

Zimbabwe: “We need a more holistic multilateral approach to technological governance given the rapid advances in technology and associated threats and risks. We urgently need a Global Digital Compact.”[156]

Finland: “One of the key focus areas of the future Summit would be agreeing on the Global Digital Compact. The Compact should add real and tangible value on how we cooperate on shared digital priorities, incentivize solutions for the benefit of SDGs, and safeguard human rights in the digital space, including privacy and the freedom of expression.”[157]

---

[149] UN Web TV, (Opening, Plenary, Closing) Preparatory ministerial meeting of the Summit of the Future - General Assembly, 78th session, 21 September 2023, (starts at: 42:52), https://media.un.org/en/asset/k1z/k1zzbbnqaq
[150] Ibid, (starts at: 1:39:10)
[151] Ibidem, (starts at: 02:55:05)
[152] Ibidem, see the original in French (starts at: 03:24:40)
[153] Ibidem, (starts at: 04:05:19)
[154] Ibidem, (starts at: 05:15:40)
[155] Ibidem, (starts at: 06:36:55)
[156] Ibidem, (starts at: 07:10:40)
[157] Ibidem, (starts at: 07:48:55)

Other UN Initiatives

Official documents of the 77th session of the U.N. General Assembly

On 15 May 2023, Russia, Belarus, North Korea, Nicaragua, and Syria (as co-sponsors) submitted the Concept of the U.N. Convention on Ensuring International Information Security as an official document of the 77th session of the U.N. General Assembly.[158]
The co-sponsors named, among others, the following principle and proposal that "could serve as the basis for the provisions of the Convention governing State activities and defining the rights and obligations of States with regard to promoting State capacity-building in the field of security in the use of information and communications technologies: [...] promotion of the development and use of secure information and communications technologies in compliance with the principle of neutrality of the global communications network, including the evolutionary reforming of protocols and information transfer methods to eliminate the possibility of using this network for criminal purposes;"[159]

Context: Russia and co-sponsors of the draft convention insisted that the draft convention concept be mentioned in the annual 2023 progress report of OEWG. Russia claimed that China and Iran also support the inclusion of the mention of the draft convention into the annual OEWG progress report.[160]

Statements by the Secretary-General's Envoy on Technology (U.N. Tech Envoy)

On 13 October 2022, U.N. Tech Envoy Ambassador Amandeep Singh Gill said: "The Summit of the Future in 2024 is an opportunity for the international community to reboot multilateralism and prepare ourselves better for the challenges of tomorrow.

The summit has been decided by the UN General Assembly on the basis of a report that the UN Secretary General was asked to present. This report is called Our Common Agenda – and the Global Digital Compact (GDC) is one of the proposals in this report. It is to be adopted at the Summit of the Future."[161]
On 24 October 2022, Ambassador Gill said: "I have no hesitation in saying that that commitment to multistakeholder approaches is very very strong. In fact when the SG spoke to the General Assembly he made it clear that either we get to the GDC through a multistakeholder process or we don't at all. It was a very very clear, very strong statement, made in New York. And we are upholding that commitment through these consultations for instance, many others, through the

[158] Ministry of Foreign Affairs of the Russian Federation, Press-release on the Concept of the U.N. Convention on International Information Security, 16 May 2023, https://mid.ru/ru/foreign_policy/news/1870609/?lang=en
[159] Updated Concept of the U.N. Convention on Ensuring International Information Security, 15 May 2023, p. 8, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ENG_Concept_of_UN_Convention__on_International_Information_Security_Proposal_of_the_Russian__Federation.pdf
[160] UN Web TV, (8th meeting) Open-ended working group on Information and Communication Technology (ICT) - Fifth Substantive Session, 27 July 2023, (starts at 13:50), https://media.un.org/en/asset/k1n/k1ngmoogyi
[161] ITU news, Establishing the Global Digital Compact: Q&A with Amandeep Singh Gill, 13 October 2023, https://www.itu.int/hub/2022/10/establishing-the-global-digital-compact-qa-with-amandeep-singh-gill/

strong engagement with not just the IGF but also other forums, – ICANN."[162] He continued: "now your question about how can we kind of go beyond the ritual of [to] essence of multi-stakeholder approaches and how can we address this thing that is either/or, – is either it's intergovernmental multilateralism or it is multi-stakeholder approaches which end up being consultative interesting discussions but what's the pathway to implementation? We struggle there and frankly no one has really cracked it."[163]
"I've heard this in New York that the WSIS Tunis formula is a good one for multi-stakeholder participation. You know that formulation within our respective mandates and authorities. I don't have the exact wording before me but for some that formula doesn't go far enough others it goes too far. So let's see where we end up with that's one of those good examples too to look at. I mentioned two recent experiences, other experiences, relatively positive: the cyber crime discussion and the ITU discussion. So maybe we can come up with a *sui generis* formula that satisfies David, Adam[164] and everyone else on this aspect".[165]

On 23 June 2023 U.N. Tech Envoy said: "I would leave you to look at, you know, the last section of this [UNSecGen] policy brief on the idea of a regular assessment of the implementation of the compact to keep pace with technology developments. And the one thing that I want to underline again, especially referring to the previous remarks in this panel – that this is a multi-stakeholder forum. So the preparation – tripartite, so those words are clearly used across civil society which includes all the actors from the technical community, Academia and the value of scientific, independent scientific expertise particularly around AI, -- you know that is clearly understood today there's private sector and there is governments."[166]

2023 Counter-Terrorism Week Side-Event

On 22 June 2023, Tech Against Terrorism, an initiative supported by the U.N. Counter-Terrorism Executive Directorate (UN CTED) called upon states to "consider ways of improving mechanisms to remove terrorist-operated websites, including helping us to intervene with domain name registrars, content distribution networks and hosting providers."[167]

Conclusion

The ongoing discussions at the United Nations in the format of OEWG will conclude in 2025, the report will serve as the outcome of these deliberations if it will be adopted as a result of the consensus. The AHC deliberations are planned to conclude in February 2024 with the adoption of the cybercrime convention by consensus or, if consensus will not be attainable, with the two-thirds majority of those country delegations voting and present. The GE function will follow and

[162] IGF, Town Hall Meeting with the UN Secretary-General's Envoy on Technology, 24 October 2022, (starts at 49:53), https://youtu.be/NEmXNzQzsCk?t=2991
[163] Ibidem, (starts at 51:31), https://youtu.be/NEmXNzQzsCk?t=3091
[164] Here, the U.N. Tech Envoy refers to the questions posed to him by the Canadian representative and MAG member on the role of the WSIS process and technical community.
[165] Ibidem, (starts at 1:06:13), https://youtu.be/NEmXNzQzsCk?t=3973
[166] YouTube Video, EuroDIG 2023 · Pre 05 | Let's promote the European vision for digital governance and cooperation, 23 June 2023, (starts at 1:36:42), https://youtu.be/RctcgFscohU?t=5802
[167] UN Web TV, Preventing and Countering the use of New and Emerging Technologies for Terrorist Purposes: Way Forward for a Holistic Multilateral Response (2023 Counter-Terrorism Week Side-Event), 22 June 2023, (starts at 1:08:27), https://media.un.org/en/asset/k1i/k1iy7ltzvt

report on both processes although it views their outcomes as likely to have zero to minimal impact on ICANN's mission.

Negotiations on the GDC will commence in January 2024, with the final stage planned to take place 20-23 September, 2024 during the Summit of the Future where the Compact is expected to be adopted on a consensus basis. Currently, this process presents too many unknowns for the organization. GE will follow all the deliberations on the GDC to report the progress and developments to the ICANN community as the dynamics of the negotiations unfold.

One World, One Internet

Visit us at **icann.org**

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

soundcloud/icann

instagram.com/icannorg