UN Update: Cyber-Related Developments

Report on cyber-related discussions at the United Nations

Veni Markovski
Alexey Trepykhalin
3 June 2021
GE-009

TABLE OF CONTENTS

Introduction

This paper provides an update of the proceedings within the different groups of the United Nations (U.N.) General Assembly (UNGA), where discussions of cybersecurity-related issues are taking place. It includes updates from the deliberations at the first Open-ended Working Group (OEWG), the Group of Governmental Experts (GGE), and the Open-ended Ad Hoc Committee of Experts (AHC[1]) between 1 July 2020 and 3 June 2021.

This paper is part of a periodic series of reports that provide an overview of activities taking place at the U.N., which are relevant to the Internet ecosystem and ICANN's mission.[2] Monitoring such activities demonstrate the commitment and responsibility of the ICANN organization's (ICANN org) Government and Intergovernmental Organizations Engagement (GE) team in keeping the broader ICANN community informed about issues of importance for the global, single, interoperable Internet, and its unique identifier system.[3]

The Open-ended Working Group (OEWG) Update

Since ICANN org's publication on cyber-related discussions at the U.N. in July 2020, the OEWG had three more rounds of informal consultations that year (29 September - 1 October, 17 - 19 November, and 1 - 3 December). During these consultations, the OEWG Secretariat received a number of comments and contributions from member states as part of the formal process, and from non-governmental organizations as part of the informal consultations initiated by the OEWG Chair.

Below, the ICANN org GE team summarizes only those contributions to the OEWG, which touch on ICANN's mission. The following is a list of those contributions sorted by date.

On 2 July 2020, the Republic of Finland: "We also wish to lend our strong support to the proposal made by the Netherlands on the protection of integrity and availability of the public core of the internet and its concrete suggestions regarding the scope of the critical infrastructure norms (13f and 13g)."[4]

On 19 November 2020, the Islamic Republic of Iran: "These [unilateral] digital sanctions have affected investment in ICT infrastructures as well as access to digital technologies, digital resources such as IPs and DNS system and networks which not only constitute

[1] In the previous two updates, we used the abbreviation OECE, but at the opening session of the committee, we noticed that the U.N. member states use another abbreviation AHC, for Ad-Hoc Committee, so for consistency ICANN org adjusted the language accordingly. Full name of this committee is "Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes".
[2] See previous reports by GE here: https://www.icann.org/resources/pages/government-engagement-publications-2020-03-02-en This and all other URLs in footnotes and appendices were retrieved on 3 June 2021.
[3] "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
[4] "Statements by the Republic of Finland" Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, Virtual Informal Consultations, 19 June and 2 July 2020, https://front.un-arm.org/wp-content/uploads/2020/09/oewg-informal-virtual-meetings-statement-by-finland-19-june-and-2-july-2020.pdf

barriers for achieving national ICT-related development goals but also violate human rights."[5]

On 19 January 2021, the Kingdom of the Netherlands: "'State and non-state actors should neither conduct nor knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace' [would be] guidance for implementation of UN GGE, 2015 recommendation 13(f) and therefore bringing this also under the scope of UN GGE 2015, recommendation 13(g)."[6]

On 19 February 2021, the Republic of Slovenia: "We would also like to support the calls made by the Netherlands for greater emphasis on the protection of the public core of the internet."[7]

On 19 February 2021, the Federal Republic of Germany: "Suggestion to include a reference to threats to the public core of the internet, as also mentioned in para 50 of the Zero Draft, in the Section on Existing and Potential Threats."[8]

On 19 - 22 February 2021, the Kingdom of the Netherlands: "Over the years, cyber-operations against the integrity, functioning and availability of the internet has shown to be a real and credible threat. This was mentioned as 'public core' in the pre-draft of the OEWG. As we are striving for consensus, we contacted the countries that had expressed concerns during our earlier discussions and came to a new wording that seems to answer the concern. It reads as follows: 'the technical infrastructure essential to the general availability or integrity of the internet.'"[9]

On 23 February 2021 the United Kingdom: "We extend our thanks to the Netherlands for working with us and others to refine their proposal on the 'public core' and welcome the inclusion of the compromise text."[10]

On 25 February 2021, the Kingdom of the Netherlands: "In line with the text on the protection of the public core that was included in the pre-draft, taking into account the convergence on the exact wording, we propose the following. We would like to propose to change the formulation in the last sentence of paragraph 21 on 'integrity, functioning and availability' to

---

[5] "The Revised "Pre-draft" of the report of the OEWG", OEWG third informal virtual meeting, Intervention by delegation of the Islamic Republic of Iran, 19 November 2020 "Capacity Building", https://front.un-arm.org/wp-content/uploads/2020/11/iran-intervention-on-capacity-building-19-nov-2020.pdf

[6] "Non-paper listing specific language proposals under agenda item "Rules, norms and principles" from written submissions by delegations", Version as of 18 January 2021, https://front.un-arm.org/wp-content/uploads/2021/01/OEWG-Non-paper-rules-norms-and-principles-19-01-2021.pdf

[7] Open-ended Working Group on developments in the field of information and telecommunications in the context of international security, Informal virtual meeting (18, 19 and 22 February 2021) Slovenia, Statement, 19 February 2021, https://front.un-arm.org/wp-content/uploads/2021/02/Slovenia-19-February-2021-FINAL.pdf

[8] Comments by Germany on the OEWG Zero Draft Report, 19 February 2021, https://front.un-arm.org/wp-content/uploads/2021/02/Germany-Written-Contribution-OEWG-Zero-Draft-Report_clean.pdf

[9] Statement by H.E. Nathalie Jaarsma, Kingdom of the Netherlands to the United Nations, (18,19, 22 February 2021), https://front.un-arm.org/wp-content/uploads/2021/02/Netherlands-OEWG-informals-intervention-Feb-2021.pdf

[10] UK Comments on the Zero Draft Report of the OEWG on Development in the Field of ICTs in the Context of International Security, 23 February 2021, https://front.un-arm.org/wp-content/uploads/2021/02/UK-submission-to-OEWG-ICTs-zero-draft-002.pdf

the [necessity of protecting] 'the technical infrastructure essential to the general availability or integrity of the internet.'"

"Additionally, we would like to mention the importance of the 'protection of the technical infrastructure essential to the general availability or integrity of the internet' under the conclusion/recommendation section of rules, norms and principles as well."[11]

On 3 March 2021, the Global Commission on the Stability in Cyberspace (GCSC): "While the Commission was very pleased to note that in the previous pre-draft report a number of the recommendations of the GCSC were considered, we regret that many of these recommendations have not been included in the zero draft or the current first draft. This particularly applies to the norm to protect the public core of the Internet, which we believe has been well received by many States, as well as civil society and private sector observers."[12]

On 8 March 2021, the Islamic Republic of Iran: "Platforms and transnational corporations like ICANN should be held accountable."[13]

On 8 March 2021, the Cybersecurity Tech Accord: "The recent SolarWinds hack has highlighted how no organization should feel immune from a sufficiently resourced and determined adversary. It also demonstrated how brazenly advanced threat actors are willing to undermine confidence in essential processes and the public core of the internet in carrying out an attack."[14]

On 9 March 2021, the Federal Republic of Germany supported the new compromised language "...in particular on the public core of the Internet."[15]

On 9 March 2021, a coalition of nine civil society organizations recommended that the OEWG report: "...reference the need for all actors to protect the basic availability and integrity of the global Internet, which includes not interfering with the public core of the Internet."[16]

On 10 March 2021, the People's Republic of China: "States should participate in the management and distribution of international Internet resources on equal footings."[17]

---

[11] The Netherlands – written proposals to OEWG zero draft, February 2021, https://front.un-arm.org/wp-content/uploads/2021/02/Netherlands-OEWG-written-comments-to-zero-draft.pdf

[12] Comments from the GCSC on the First Draft of the Substantive Report of the Open-ended Working Group, 3 March 2021, https://front.un-arm.org/wp-content/uploads/2021/03/GCSC-Submission-to-OEWG-First-Draft-Report-March-2021.pdf

[13] 1st meeting - Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, Third Substantive session (8-12 March 2021), UN Web TV, 8 March 2021, (starts at 1:29:40) https://media.un.org/en/asset/k1o/k1obxycc3u

[14] Cybersecurity Tech Accord Response to the UN-OEWG's Substantive Report [FIRST DRAFT], https://front.un-arm.org/wp-content/uploads/2021/03/Tech-Accord-OEWG-response-March-2021-FINAL.pdf

[15] 3rd meeting - Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, Third Substantive session (8-12 March 2021), UN Web TV, 9 March 2021, (starts at 38:20), https://media.un.org/en/asset/k13/k13uzdidth

[16] "Joint Civil Society Feedback on First Draft of the OEWG on ICTs Report," OEWG documents' depository, 9 March 2021, https://front.un-arm.org/wp-content/uploads/2021/03/Joint-CS-feedback-on-first-draft-1.pdf

[17] Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, Third substantive session, 8–12 March 2021, OEWG Chair's

On 12 March 2021, the GCSC expressed its "regret that the term public core was not reflected in the final draft of the OEWG report."[18]

In addition to the release of the OEWG final report, the OEWG Chair published a Chair's summary, which included the earlier wording on the public core, as proposed by the Netherlands on 19 January.[19]

The compromise language of the 2021 OEWG final report, with the new wording as agreed upon between member states, reads in points 18 and 26, as follows:

"18. States concluded that there are potentially devastating security, economic, social and humanitarian consequences of malicious ICT activities on critical infrastructure (CI) and critical information infrastructure (CII) supporting essential services to the public. While it is each State's prerogative to determine which infrastructures it designates as critical, such infrastructure may include medical facilities, financial services, energy, water, transportation and sanitation. 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. Such infrastructure may be owned, managed or operated by the private sector, may be shared or networked with another State or operated across different States. As a result, inter-State or public-private cooperation may be necessary to protect its integrity, functioning and availability."[20]

"26. While agreeing on the need to protect all critical infrastructure (CI) and critical information infrastructure (CII) supporting essential services to the public, along with endeavouring to ensure the general availability and integrity of the Internet, States further concluded that the COVID-,19 pandemic has accentuated the importance of protecting healthcare infrastructure including medical services and facilities through the implementation of norms addressing critical infrastructure, such as those affirmed by consensus through UN General Assembly resolution 70/237."[21]

The delegation of the Netherlands, in its comments on the OEWG consensus report, noted that "the Netherlands warmly welcomes the inclusion of the general availability and integrity of the Internet, - what we see as the public core of the Internet."[22]

Summary, Conference room paper, 10 March 2021, A/AC.290/2021/CRP.3*, https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf

[18] Statement from the GSCS on the final draft of the substantive report of the UN Open-Ended Working Group, 12 March 2021, https://front.un-arm.org/wp-content/uploads/2021/03/GCSC-Statement-OEWG-Multistakeholder-Consultation-Final-Draft-Report-March-2021.pdf

[19] Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, Third substantive session, 8–12 March 2021, Chair's Summary, Conference room paper, 10 March 2021, A/AC.290/2021/CRP.3*, https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf

[20] Open-ended working group on Developments in the Field of Information and Telecommunications in the Context of International Security, Final Substantive Report Conference room paper, 10 March 2021, A/AC.290/2021/CRP.2, https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

[21] Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, Final Substantive Report, Conference room paper, 10 March 2021, A/AC.290/2021/CRP.2.

[22] 9th meeting - Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, Third Substantive session (8-12 March 2021), UN Web TV, 12 March 2021, (starts at 35:23), https://media.un.org/en/asset/k1r/k1rf2exuhz

The Group of Governmental Experts (GGE) Update

On 28 May 2021, the consensus report of the GGE was adopted.[23] Several points in the report are relevant for the ICANN community, within the global context of cyber-related deliberations at the U.N. that we have witnessed in the last few years. The quoted points listed below (in some cases quoted partly) are taken from the *Advance Copy Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security* and the report's "Letter of transmittal."[24]

Point 10: "Harmful ICT activity against critical infrastructure that provides services domestically, regionally or globally, which was discussed in earlier GGE reports, has become increasingly serious. 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."

Point 17: "The Group also noted the proposal of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan for an international code of conduct for information security (see A/69/723)."[25]

Point 44: "As noted in norm 13 (g), States should take appropriate measures to protect their critical infrastructure. In this regard, each State determines which infrastructures or sectors it deems critical within its jurisdiction, in accordance with national priorities and methods of categorization of critical infrastructure."

Point 45: "Critical infrastructure may also refer to those infrastructures that provide services across several States such as the technical infrastructure essential to the general availability or integrity of the Internet."

Point 48: "A State's designation of an infrastructure or sector as critical can be helpful for protecting said infrastructure or sector. In addition to determining the infrastructures or sectors of infrastructure it deems critical, each State determines the structural, technical, organizational, legislative and regulatory measures necessary to protect their critical infrastructure and restore functionality if an incident occurs."

Point 49: "Some States serve as hosts of infrastructures that provide services regionally or internationally. ICT threats to such infrastructure could have destabilizing effects. States in such arrangements could encourage cross-border cooperation with relevant infrastructure owners and operators to enhance the ICT security measures accorded to such infrastructure and strengthen existing or develop complementary processes and procedures to detect and mitigate ICT incidents affecting such infrastructure."

---

[23] Twitter message by the US Department of State, 28 May 2021, https://twitter.com/State_Cyber/status/1398314450743091201?s=20

[24] Advance Copy, Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security and Letter of transmittal, 28 May 2021, https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf

[25] Annex to the letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General [Original: Chinese and Russian], International code of conduct for information security, A/69/723, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/014/02/PDF/N1501402.pdf?OpenElement

Point 63: “In addition, and in consultation with relevant industry and other ICT security actors, States can develop guidance and incentives, consistent with relevant international technical standards, on the responsible reporting and management of vulnerabilities and the respective roles and responsibilities of different stakeholders in reporting processes; the types of technical information to be disclosed or publicly shared, including the sharing of technical information on ICT incidents that are severe; and how to handle sensitive data and ensure the security and confidentiality of information.”

Point 79: “Dialogue through bilateral, sub-regional, regional and multilateral consultations and engagement can advance understanding between States, encourage greater trust and contribute to closer cooperation between States in mitigating ICT incidents, while reducing the risks of misperception and escalation. Other stakeholders such as the private sector, academia, civil society and the technical community can contribute significantly to facilitating such consultations and engagement.”

Point 87: “The Group underscores the importance of cooperation and assistance in the area of ICT security and capacity-building and their importance to all elements of the Group’s mandate. Increased cooperation alongside more effective assistance and capacity-building in the area of ICT security involving other stakeholders such as the private sector, academia, civil society and the technical community can help States apply the framework for the responsible behaviour of States in their use of ICTs. They are critical to bridging existing divides within and between States on policy, legal and technical issues relevant to ICT security. They may also contribute to meeting other objectives of the international community such as the SDGs.”

Point 95: “The Group also identified potential areas for future work, which include but are not limited to:[...] (d): “Identifying mechanisms that facilitate the engagement of other essential stakeholders, including the private sector, academia, civil society and the technical community in efforts to implement the framework of responsible behaviour, where appropriate.”

The Open-Ended Ad Hoc Committee of Experts (AHC) Update

The AHC was scheduled to start its work in August 2020, but due to the COVID-19 pandemic, its first organizational session took place from 10 - 12 May 2021.[26] Since ICANN org’s July 2020 paper, there have been some new contributions published on the AHC webpage.[27] At the first meeting of its organizational session held on 10 May 2021, the AHC elected the Chair of the Committee, its Rapporteur, and 13 Vice-Chairs, representing

[26] The meetings of the organizational session of the AHC can be viewed here:
First meeting: https://media.un.org/en/asset/k1v/k1vgo4a624 (The second meeting did not take place because all organizational issues were resolved during the first meeting)
Third meeting: https://media.un.org/en/asset/k1z/k1zsp4exqc
Fourth meeting: https://media.un.org/en/asset/k12/k12bsxlcak
Fifth meeting: https://media.un.org/en/asset/k1m/k1ma80pf1p
Sixth meeting: https://media.un.org/en/asset/k1m/k1m0si6d6n

[27] “Ad hoc committee established by General Assembly resolution 74/247”, UNODC, https://www.unodc.org/unodc/en/cybercrime/cybercrime-adhoc-committee.html

different geographical regions.[28] The AHC failed to reach a consensus on the organizational modalities of its future meetings during the allotted time, and the Chair announced that informal consultations would follow.[29]

On 26 May 2021, at its 71st plenary meeting, the U.N. General Assembly adopted, without a vote, the text of the resolution A/RES/75/282 "Countering the use of information and communications technologies for criminal purposes."[30] The documents established two locations for the AHC sessions – Vienna and New York City. A total number of seven sessions will be held and the location of these sessions will rotate between Vienna and New York City. The first and last sessions will take place at the U.N. in New York City. Decisions of the AHC on substantive matters without approval by consensus, shall be taken by a two-thirds majority of the representatives present and voting.

The resolution also encourages the chair of the AHC to host intersessional consultations to solicit inputs from a diverse range of stakeholders on the elaboration of the draft convention.

Conclusion

The GE team will continue to monitor discussions at the AHC and the new OEWG, which will perform its work from 2021 to 2025. This OEWG held its first organizational meeting on 1 June 2021, during which it elected the Permanent Representative of Singapore to the U.N. as the Chair.[31]

Updates on the work of the OEWG, GGE, AHC, as well as other GE publications may be found on ICANN org's GE webpage.[32]

[28] The organizational session of the Ad Hoc Committee was held in New York, on 10-12 May 2021, Results of the elections of the Ad Hoc Committee https://www.unodc.org/unodc/en/cybercrime/cybercrime-adhoc-committee.html

[29] 6th meeting, Ad Hoc Committee to Elaborate a Comprehensive International Convention on Cybercrime, Un Web TV, 12 May 2021, (starts at 3:24:34) https://media.un.org/en/asset/k18/k18lkzt0oq

[30] Resolution adopted by the General Assembly on 26 May 2021, "75/282. Countering the use of information and communications technologies for criminal purposes", Distr.: 1 June 2021, A/RES/75/282, https://undocs.org/a/res/75/282

[31] 1 June, 1st meeting: https://media.un.org/en/asset/k1o/k1oa2ngbsc
1 June, 2nd meeting: https://media.un.org/en/asset/k14/k1443my9hu

[32] GE webpage, ICANN website: https://www.icann.org/resources/pages/government-engagement-publications-2020-03-02-en

Appendix

OEWG. Final Substantive Report: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

OEWG. Chair's Summary: Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security Third substantive session 8–12 March 2021
https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf

OEWG. Video footage of the third substantive meeting, 8-12 March 2021

8 March 2021
Day 1: 1st meeting
https://media.un.org/en/asset/k1o/k1obxycc3u

Day 1: 2nd meeting
https://media.un.org/en/asset/k18/k1893g1q0h

9 March 2021
Day 2: 3rd meeting
https://media.un.org/en/asset/k13/k13uzdidth

Day 2: 4th meeting
https://media.un.org/en/asset/k1h/k1huoxryeo

10 March 2021
Day 3: 5th meeting
https://media.un.org/en/asset/k1d/k1d4e06j0x

Day 3: 6th meeting
https://media.un.org/en/asset/k1m/k1mqlxrfv4

11 March 2021
Day 4: 7th and 8th meetings did not take place. The day was dedicated to bilateral discussions and consultations with capitals.

12 March 2021
Day 5: 9th meeting
https://media.un.org/en/asset/k1r/k1rf2exuhz

Day 5: 10th meeting (The U.N. website does not provide a link to the recording of this session).

Day 5: 11th meeting, final OEWG session (adoption of the substantive report by consensus)
https://media.un.org/en/asset/k1p/k1prn29un6