United Nations Update: Cyber-Related Discussions

ICANN Government & Intergovernmental Organization (IGO) Engagement

Veni Markovski
GE-005
15 July 2020

TABLE OF CONTENTS

Foreword

This paper provides an update of the proceedings within the working groups of the United Nations General Assembly (UNGA), where discussions of Internet- and cybersecurity-related issues take place.

During these discussions, issues that touch on ICANN's mission are raised every once in a while, and they might continue to be mentioned in the future. Monitoring the discussions is part of how ICANN organization's Government Engagement (GE) function supports ICANN's mission, and also shows GE commitment and responsibility to keep the broader ICANN community informed about issues of importance for the global, single, interoperable Internet and its unique identifier system.[1]

In our previous paper, "Brief Overview of UN Deliberations on Cybersecurity and Cybercrime", we provided the information about the establishment of the different working groups and processes at the United Nations (UN).[2] In this paper, we are focusing on updates on the Open-ended Working Group (OEWG) and the Open-ended ad hoc intergovernmental committee of experts (OECE).

[1] As explained in our five year operating and financial plan, p.47: "Monitor legislation, regulation, norms, principles, and initiatives that may impact ICANN's mission"
[2] This paper is part of a series published by Government Engagement starting 28 February 2020. For all Government Engagement papers, please visit our webpage here.

Updates on OECE, OEWG, and GGE

OECE

The OECE[3] began its work on "countering the use of information and communications technologies for criminal purposes" with the publication of a document containing a proposed outline and modalities for the next four years.[4] The document, slated for discussion during the first meeting of the group in August 2020, provides a framework for the work of the OECE until its conclusion in June 2024.

On July 10, a virtual informal meeting related to the Cybercrime Ad Hoc Committee organizational session took place. During the meeting, UNODC provided an update on the procedural issues related to the August organizational session of the ad hoc committee, and then member states discussed the provisional agenda for the organizational session of the ad hoc committee.[5] More information about this July virtual informal meeting can be found on the OECE website, in particular in the document titled "Summary of information provided by the DTA Director, UNODC, at the informal meeting on 10 July 2020."[6]

As of 13 July 2020, the OECE has published on their webpage comments from the following member states: Australia, Canada, Dominican Republic, European Union, Islamic Republic of Iran, Japan, Russian Federation, United Kingdom of Great Britain and Northern Ireland, and the United States of America.

OEWG

Since March 2020, the OEWG[7] Chair published an initial pre-draft report on 11 March 2020.[8] This document was open for comments by all stakeholders with the intention for it to be discussed during a face-to-face meeting at the end of March 2020. However, due to COVID-19, that meeting did not take place.[9] Instead, the member states were invited to send written comments. Dozens of member states, intergovernmental organizations, and nongovernmental organizations sent their comments, which were published on the group's website.[10]

In this paper, we quote some of the comments submitted in response to the Chair's call for comments.[11] We focus only on the comments which might be interpreted as touching on ICANN's mission or remit.

---

[3] OECE stands for Open-ended ad hoc intergovernmental committee of experts; it consists of all UN Member States and is tasked with drafting a new UN cybercrime convention. In this paper we use the term "cybercrime convention," the UN however uses "comprehensive international convention on countering the use of information and communications technologies for criminal purposes."
[4] The document can be found here.
[5] UN Office on Drugs and Crime, https://www.unodc.org/
[6] Download PDF here.
[7] OEWG stands for Open-ended Working Group on developments in the field of information and telecommunications in the context of international security; we use the term cybersecurity in our paper.
[8] Download the PDF here.
[9] Note: COVID-19 has impacted the usual functioning of the UN and the above-mentioned working groups. For instance, the OEWG had the first round of its virtual informal meetings in June and July 2020.
[10] https://www.un.org/disarmament/open-ended-working-group/
[11] See the invitation here.

***

Point 38 of the pre-draft report starts with:

"*States, during discussions and through written submissions, also proposed suggestions for the 'upgrading' as well as further elaboration of norms. Proposals included, inter alia, that States should affirm their commitment to international peace and security in the use of ICTs; that it should be reaffirmed that States hold the primary responsibility for maintaining a secure, safe and trustable ICT environment; that the general availability or integrity of the public core of the Internet should be protected; [...cut...]".*

Comments by some member states (in alphabetical order) on the pre-draft report

Brazil: "*From the point of view of Brazil, the IT infrastructures underpinning electoral processes also deserve the same protection accorded to the public core of the Internet (paragraph 38)."*

China: *"Given the limited amount of time we have, attention should also be drawn to avoid introducing concepts that have not gained global consensus yet ("public core" for instance) into the report."*
and: *"During the previous two sessions, parties including China have put forward dozens of constructive proposals on issues such as cyber sovereignty, supply chain security, protection of critical infrastructure, refraining from unilateral sanction and fight against cyber terrorism. It is hoped that these proposals could be incorporated in the report."*

Egypt: "*Member States should be encouraged to reach an agreed common definition of what constitutes "critical infrastructure", with a view to agreeing, as appropriate, on prohibiting any act that knowingly or intentionally utilizes offensive ICT capabilities to damage or otherwise impair the use and operation of critical infrastructure.*"

Germany: *"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)*
and: *"Regarding paragraph 31, Germany would like to emphasize that the focus of the OEWG should be on enhancing existing norms and improving their understanding and implementation. In this regard we consider the proposals to protect the public core of the internet, not to disrupt the infrastructure essential to political processes, not to harm medical facilities and to highlight transnational infrastructure as useful additions to the already existing norms on the protection of critical infrastructure as contained in the 2015 GGE report."*

Iran: *"The pre-draft has, however, failed to acknowledge some important corresponding threats, including unilateral coercive measures, monopoly in Internet governance, anonymity of persons and things, offensive cyber strategies and policies, etc., which clearly affect awareness, resilience and capacities of the countries."*

The Netherlands: *"To address these threats, the Netherlands would like to suggest that the OEWG considers the recommendation that "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" as 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)."
and: *"The Netherlands would like to suggest for the report of the OEWG to consider the threat that cyberoperations pose against the general availability or integrity of the public core of the Internet. Over the years, cyber operations against the integrity, functioning and availability of the internet has shown to be a real and credible threat."*

Nicaragua: notes the current *"insufficient regulation of the private sector activities in the field of ICT"* are a *"major threat for the development of a peaceful environment of ICTs."*

Pakistan: *"Member States should be encouraged to arrive at an agreed common definition of what constitutes "critical infrastructure", with a view to agreeing on the prohibition of ICT activity that knowingly or intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure."*

Russia: *"The importance of "multi-stakeholder approach" with emphasis on the contribution of non-governmental sector, business and academia to ensuring responsible behaviour in the information space is artificially exaggerated. At the same time the problem of insufficient regulation of private sector activities in the ICT sphere and increasingly urgent issue of monopolization of this area is omitted as one of the key threats to the development of peaceful and competitive ICT environment."*

Switzerland: *"For example, proposals relating to the protection of the public core of the internet, not to harm medical facilities, not to disrupt infrastructure essential to political processes and relating to transnational critical infrastructure could in our view provide valuable guidance to existing norms."*

USA: *"...selective elaboration of norms or identification of specific critical infrastructure sectors carries some risk of giving precedence to certain issues over others."*

European Union: *"Therefore, the protection of critical infrastructure is of such importance, that the EU and its Member States would suggest for the OEWG report to consider these threats, including the one posed against the general availability or integrity of the public core of the Internet."*

Comments by nongovernmental organizations

Global Partners Digital: *"Recommendation: We support the recommendations by the Netherlands in the "non-paper", to elaborate on and provide further guidance on norms (f) and (g) in the UN GGE 2015 report (Res 70/237)—namely that "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."*

Internet Society: *"The Internet's public core encapsulates the Internet routing, naming and numbering systems (the Domain Name System), security and identity cryptography mechanisms, and communications cables. These are the core functions that make the Internet work and should be safeguarded to ensure that the Internet remains an enabling technology that has global reach and integrity. We encourage the OEWG to take due cognizance of the values of the GCSC Norm to Protect the Public Core, which emphasizes the need for both state and non-state*

actors to refrain from allowing any activity that could intentionally or substantially damage the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace."

Microsoft: in its first submission says, *"strongly supports several of the new norms that have been proposed by Member States which we believe are critical additions to the existing foundation of cyber norms previously agreed in the GGE context: 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."* Microsoft also calls on members to follow the Paris Call principle to *"Prevent activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet."*

Microsoft, in a second submission, states *"Previous GGE commitments reflect this importance, and various statements since, including the Paris Call and the GCSC, reflect growing commitment to protect the technology that constitutes the backbone of internet itself from cyberattacks. Some efforts refer to this as protecting the general availability or integrity of the "public core" of the Internet, with some preferring reference to technical components of the internet. Importantly, states should agree on a new norm to protect those central components without which the global Internet would cease to operate. The GCSC defines these components as: packet routing and forwarding; naming and numbering systems; cryptographic mechanisms of security and identity; transmission media, software and data centers."*

Twelve NGOs[12] issued a joint statement: *"Attacks on critical infrastructure, and here also on "supranational critical information infrastructure" (which should be understood to include the Domain Name System and other elements of the public core of the Internet), pose not only "a threat to security but also to economic development and people's livelihoods" (paragraph 19). We suggest that this human cost of attacks on critical infrastructure and their impact on human rights be directly and clearly referred to in the report."*
and *"We support the recommendation in paragraph 38 that the general availability or integrity of the public core of the Internet should be protected, which should be understood as further specification or elaboration of the already agreed 2015 GGE norms to protect critical infrastructure. Public core refers to critical elements of the infrastructure of the Internet, namely packet routing and forwarding, naming and numbering systems, the cryptographic mechanisms of security and identity, transmission media, software, and data centers."*

***

On 27 May 2020 the Chair of the OEWG published[13] a revised pre-draft report and an updated non-paper[14]which reflect, per the Chair's letter, the "new proposals received under the agenda item 'Rules, norms and principles'".[15] This updated pre-draft report and the non-paper were discussed in a virtual meeting, which took place on 15, 17, 19 June and 2 July

[12] These 12 NGOs are: Access Now, Association for Progressive Communications, Centre for Communication Governance at National Law University Delhi, Derechos Digitales, Fundación Karisma, Global Partners Digital, Kenya ICT Action Network (KICTANet), International Center for Not-for-Profit Law, R3D: Red en Defensa de los Derechos Digitales, Research ICT Africa, Media Foundation for West Africa, YMCA computer training centre and digital studio, the Gambia.
[13] https://front.un-arm.org/wp-content/uploads/2020/05/200527-oewg-ict-revised-pre-draft.pdf
[14] https://front.un-arm.org/wp-content/uploads/2020/05/200527-oewg-ict-non-paper.pdf
[15] The letter is published here.

2020. According to a letter published on 16 July2020 by the Chair of the OEWG and the Permanent Representative of Switzerland to the UN, Ambassador Jürg Lauber, the schedule for the next informal meetings to discuss the pre-draft is as follows: second round 29 September–1 October 2020; third round 17–19 November 2020; and the fourth round 1–3 December 2020.[16]

The second round will discuss issues of international law; the third will look at confidence-building measures and capacity building; and the fourth will consist of regular institutional dialogue and general comments. Following this, the Chair is expected to publish a Zero Draft report (in the beginning of 2021), which will be discussed during the third substantive meeting on 8-12 March 2021. As of the time of the Chair's letter, the plan is for the informal meetings to be virtual or hybrid and the substantive meeting to be physical.

Group of Government Experts (GGE)

There's no new update on the work of the GGE since the information in our paper from 28 February 2020.[17]

ICANN Engagement and Next Steps

The ICANN org GE team organized and co-hosted a virtual briefing for diplomats from the Permanent Missions to the UN on 22 April 2020. The briefing was co-hosted by the Permanent Missions of Bulgaria and Estonia to the UN in New York and by the UN Office in Geneva. ICANN's Chief Technology Officer, David Conrad, and Naela Sarras, Senior Manager, IANA Services, spoke and interacted with the 116 diplomats who participated. They explained ICANN's role in the Internet ecosystem and addressed questions submitted by the diplomats.

The ICANN GE team will continue to follow the deliberations at the UN and will publish necessary updates, as appropriate.

[16] The letter can be downloaded (PDF) here.
[17] https://www.un.org/disarmament/group-of-governmental-experts/

ANNEX 1

Background Information about the UN and the UNGA Committees

Founded on 24 October 1945, the UN is recently becoming more involved in discussions which include different Internet-related issues. The UNGA has been deliberating for years resolutions within its First and Second Committees, aimed at cybersecurity and Internet governance (IG).[18]

UNGA First Committee[19] is the committee which historically started the discussion of the first cyber-related resolution.[20] In 2018, it established two working groups on cybersecurity – the OEWG[21] and GGE, which have been addressed in the paper published in February 2020.[22]

UNGA Second Committee[23] addresses Internet-related issues within the resolution on Information and Communication Technologies (ICT) for development.[24] The IG-related discussions started[25] with the 2002 UNGA resolution A/RES/56/183[26] during the World Summit on the Information Society (WSIS). That resolution was updated several times in 2003 and 2005, in preparation for the WSIS in Geneva (2003) and Tunis (2005). Between the Geneva and the Tunis phases of the WSIS, a Working Group on Internet Governance (WGIG) was established, which publishedits own report.[27]

The WSIS passed a document, the WSIS Tunis Agenda, which has served since 2005 as one of the key documents explaining (among many other issues) the multistakeholder model of Internet governance.[28]

The UNGA Second Committee annually reviews the ICT for development resolution. In 2015 it also spent a substantial amount of time within the *WSIS+10* deliberations, which resulted with the publication of the WSIS+10 Outcome Document[29] and culminated in a High-Level UNGA meeting on 15-16 December 2015.[30] The Outcome Document, among others, reconfirmed the multistakeholder model of Internet governance, and extended the Internet Governance Forum (IGF) for another ten year period.[31]

---

[18] As explained above, the UN doesn't use the term "cybersecurity," but we do for the information purpose of this paper.
[19] http://www.un.org/en/ga/first/index.shtml
[20] A/RES/53/70, titled "Developments in the field of information and telecommunications in the context of international security", was proposed in 1998.
[21] The OEWG is for "developments in the field of information and telecommunications in the context of international security."
[22] https://www.icann.org/resources/pages/government-engagement-publications-2020-03-02-en
[23] https://www.un.org/en/ga/second/index.shtml
[24] Since 2018, ICT for sustainable development, as seen on the UNCTAD website.
[25] The WSIS was first discussed by the ITU at its 1998 Plenipotentiary Conference, and its decision to hold the WSIS was endorsed by the UNGA in 2001.
[26] https://unctad.org/en/PublicationsLibrary/ares56d183_en.pdf
[27] See it at the US State Department or download the PDF from the WGIG site itself.
[28] https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html
[29] The UN site is not working, but the document can be found by search of its name: UNPAN95735.pdf
[30] Official website: https://publicadministration.un.org/wsis10/GA-High-Level-Meeting
[31] https://www.intgovforum.org/multilingual/

The **UNGA Third Committee**[32] started looking into cybercrime, with a resolution[33] from 2019, creating the Open-ended ad-hoc intergovernmental committee of experts (OECE) to start drafting a new UN cybercrime convention.[34]

[32] https://www.un.org/en/ga/third/index.shtml
[33] Download it in one of the UN languages here.
[34] The full name of this group is “open-ended ad hoc intergovernmental committee of experts, representative of all regions, to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes.”