29 November 2019

DISCUSSION PAPER ON INTERNATIONAL CYBERSECURITY NORMS
UN Open-ended Working Group on developments in the field of information and telecommunications in the context of international security
(December 2019 Intersessional)

I. Introduction

In September, the United Nations open-ended working group on developments in the field of information and telecommunications in the context of international security (OEWG) had its first substantive meeting in New York. Despite some diverging views among states, many state representatives highlighted the need to focus on common interests. The pressing need to make progress on international cybersecurity norms remains clear. States can take many steps domestically to advance better cybersecurity that centers and protects individuals while safeguarding human rights. However, many common interests cannot be achieved by any one state alone, and require further discussion and work as an international community.

Developments in the field of information and telecommunications (ICTs) in the context of international security have been on the UN agenda since 1998. Upon recommendation of the First Committee, the General Assembly adopted its first resolution on this issue in January 1999. Resolution 53/70 and subsequent resolutions all express two major concerns: First, the maintenance of international stability and security.[1] And second, the effects that the use of ICTs may have on the interests of the entire international community.

The concerns were important enough for the General Assembly to request regular reports on this issue by the Secretary-General. The General Assembly mandated the Secretary-General to write these reports with the assistance of a group of governmental experts (GGE).[2] Pursuant to this request the Secretary-General established the first GGE in 2004[3] with the mandate to

- consider existing and potential threats in the sphere of information security
- identify possible cooperative measures to address them, and
- study relevant international concepts *aiming to strengthen the security of global information and telecommunications systems*.[4]

The mandate of subsequent GGEs were framed along the same lines.[5] The GGE has adopted three consensus reports in 2010, 2013 and 2015. Most importantly, the 2013 report determines the

[1] G.A. Res. 53/70, U.N. Doc. A/RES/53/70 (January 4, 1999).
[2] G.A. Res. 56/19, U.N. Doc. A/RES/56/19 (January 7, 2002); G.A. Res. 57/53, U.N. Doc. A/RES/57/53 (December 30, 2002); G.A. Res. 58/32, U.N. Doc. A/RES/58/32 (December 18, 2003).
[3] G.A. Res. 59/61, U.N. Doc. A/RES/59/61 (December 16, 2004).
[4] G.A. Res. 58/32, U.N. Doc. A/RES/58/32 (December 18, 2003).
[5] G.A. Res. 60/45, U.N. Doc. A/RES/60/45 (December 8, 2005); G.A. Res. 66/24, U.N. Doc. A/RES/66/24 (December 2, 2011); G.A. Res. 68/243, U.N. Doc. A/RES/68/243 (December 27, 2013); G.A. Res. 70/237, U.N. Doc. A/RES/70/237 (December 23, 2015).

applicability of international law to the ICT environment[6]. The 2015 report further includes a list of eleven voluntary, non-binding norms of responsible behavior of states, and confidence building measures[7].

Access Now is an international organization that defends and extends the digital rights of users at risk around the world. As part of this mission we operate a global Digital Security Helpline for users at risk to mitigate specific technical threats. We work directly with policymakers and regulators at national and international forums to ensure policy decisions are focused on users and those who are most vulnerable. We also host RightsCon, the world's leading conference on human rights in the digital age. Access Now, through its Digital Security Helpline, is a member of the Forum for Incident Response (FiRST), the leading global incident response network. We are founding members of CiviCERT, a coordinating network of help desks for civil society whose goal is to improve the incident response capabilities of its members and share information on threats that affect NGOs, journalists, and other human rights defenders around the world. We support emerging regional and community-based help desk efforts to further close the gap between those in need and mechanisms of support.

As the UN Secretary-General said at the 2019 Internet Governance Forum, "We have a collective responsibility to give direction to these technologies so that we maximize benefits and curtail unintended consequences and malicious use, and so far we have not kept pace."[8] Based on our experiences and those of the wider digital security community, our overall view on global cybersecurity discussions is to encourage governments participating in all such processes to follow three principles:

> Put users at the center of cybersecurity policy
> Apply systemic solutions to systemic problems such as digital security threats
> Use open and pluralistic processes to develop cybersecurity policy

Access Now welcomes the progress that has been made in identifying norms to maintain international stability and security in the context of ICTs. However, Access Now believes that the current norms require further development, as well as enhanced collaboration, capacity building, and enforcement, to address existing threats in the sphere of information security. Some of the existing norms should also be clarified in order to facilitate their operationalization. In our view, the lack of ability, motivation, and accountability that states and companies exhibit with regard to the increasing attacks on at-risk users, and the insecurity that pervades the ICT sector generally, require urgent action by all stakeholders. Indicators from declining Freedom on the Net,[9] to increasing internet shutdowns,[10] to proliferation of spyware,[11] as well as attacks on infrastructure,[12] show the need for

[6] G.A. Res. 68/98, U.N. Doc. A/RES/68/98 (June 24, 2013).
[7] G.A. Res. 70/174, U.N. Doc. A/RES/70/174 (July 22, 2015).
[8] https://www.un.org/sustainabledevelopment/blog/2019/11/igf-internet-as-force-for-good/
[9] https://www.freedomonthenet.org/report/freedom-on-the-net/2019/the-crisis-of-social-media
[10] https://accessnow.org/keepiton

concerted efforts like these working groups undertake to build norms on responsible state behavior.

In 2017, the GGE failed to produce a consensus report,[13] though its recommendations have been endorsed by regional fora, including ASEAN.[14] Subsequently, two different processes were established at the UN to discuss issues related to ICT security: a new GGE including 25 member states and submitting a final report to the General Assembly in 2021,[15] and a new Open-ended Working Group open to all member states and reporting back to the General Assembly in 2020.[16]

This discussion paper gives an overview on the motivation of states to participate in the debate on international norms in the ICT environment and the direct objectives of existing norms. This outline is primarily based on the GGE consensus reports as well as the mandate of the new GGE and the OEWG.

II. The Goals of the International Cybersecurity Norm Debate

In order to have a fruitful debate on international cybersecurity norms, Access Now believes that it is crucial to understand the motivation of governments to agree on norms and to identify the concrete objective of agreed norms.

Governments have different motivations to participate in the debate on international cybersecurity norms. The OEWG and the GGE mandates all call for the peaceful use of ICTs and the *promotion of international peace, security and stability* in the ICT environment. Similarly, the mandates call for possible strategies to address emerging threats, consistent with the need to *preserve the free flow of information*.

These goals are important and international efforts are crucial to achieve them. Access Now, however, encourages states to elaborate additional goals. The use of ICTs for the common good of humankind (OEWG) or the common good of states (GGE) have been mentioned in the respective documents. Access Now encourages governments to think about these goals in further depth, with understanding of the broad and expanding role of ICTs in the security of modern societies.

Finally, the trustworthiness of ICT systems should be elaborated. The voluntary, non-binding norms in the GGE report 2014/ 2015 refer to the end user's confidence in the security of ICT products. It is, however, only mentioned as an objective for measures that should be taken regarding the supply

[11] See e.g. https://www.accessnow.org/export-bans-wont-stop-surveillance-we-need-a-new-global-approach; https://www.accessnow.org/new-report-shows-100-members-of-civil-society-targeted-as-nso-group-continues-to-evade-scrutiny/

[12] https://www.accessnow.org/its-not-the-first-time-iran-has-shut-down-the-internet-but-this-time-its-different/

[13] GGE report, U.N. Doc. A/72/327 (August 14, 2017).

[14] Chairman's Statement of the 3rd ASEAN Ministerial Conference on Cybersecurity Singapore (September 19, 2019)

[15] Established by G.A. Res. 73/266, U.N. Doc. A/RES/73/266 (December 22, 2018).

[16] Established by G.A. Res. 73/27, U.N. Doc. A/RES/73/27 (December 5, 2018).

chain of these products, ignoring their intended and actual impacts.[17]

Access Now believes that it is important to focus on the *trust by users and technologists* in a more comprehensive manner. This belief is supported by a number of multilateral declarations already calling for a broader consideration of trust in debates on international cybersecurity norms. The G7 Biarritz Strategy and the G20 Osaka Leaders' Declaration, both published in 2019, highlight the importance to strengthen trust in the ICT environment.

III. The Promotion of an Open, Secure, Stable, Accessible, Peaceful, Safe and Reliable ICT environment

The objective of international norms in the ICT environment is the promotion of an open, secure, stable, accessible and peaceful ICT environment. This objective is determined in the GGE reports from 2013 and 2015.[18] The conclusions of both reports have been confirmed by the mandate of the OEWG in resolution 73/27.

Access Now welcomes these objectives as a basis for future discussions on international norms in the ICT environment. We note that other multilateral declarations highlight similar objectives. The G7 Biarritz Strategy, for example, promotes an open, free, and secure digital transformation. With a slightly different focus, the G20 Osaka Leaders' Declaration declares a commitment to achieve an inclusive, sustainable, safe, trustworthy and innovative society through digitalization and promoting the application of emerging technologies. This declaration, drafted by Japan, focuses on social well-being and a human-centered digital society.

Access Now notes that some stakeholders may contest whether there is a globally recognized definition of an open, secure, stable, accessible and peaceful ICT environment. We believe that the objective of international norms in the ICT environment should be interpreted with the interest of states, societies, and humans in mind, and attention to at-risk individuals and communities. Building upon this belief we promote an open, secure, stable, accessible, peaceful, safe and reliable ICT environment and argue that international norms should aim to achieve these objectives in a human rights-respecting manner.

It is important to highlight that the concepts of safety and reliability have not yet been included in previous GGE reports. The mandate of the OEWG and the mandate of the GGE 2019/2020, however, mention the need to strengthen a reliable ICT environment.

IV. Access Now's recommendations for OEWG participants

The GGE reports, the mandates of the OEWG and the new GGE as well as other multilateral documents demonstrate the evolution and shift of the debate on international norms. The debate has

[17] GGE report, U.N. Doc. A/70/174 (July 22, 2015) para. 13 (i).
[18] GGE report, U.N. Doc. A/70/174 (July 22, 2015) para. 13; GGE report, U.N. Doc. A/68/98 (June 24, 2013) para. 19.

moved from a focus on the stability and security among states in their international relations to an inclusion of the interests of end users and societies. Access Now welcomes the references to user trust in ICT systems and hopes that future debates will strengthen human-centered norms.

To support the productive environment during the first substantive meeting of the OEWG, Access Now proposes the following initial recommendations, which we will review and update as required based on the discussions during and subsequent to the December 2019 OEWG intersessional meeting:

1. **Defining the Objective of International Cybersecurity Norms**

   The OEWG should further clarify the objective that shall be achieved by the agreed voluntary, non-binding norms. The objectives might not be limited to those already mentioned in the GGE reports. Influence could be derived from other multilateral declarations and governance of new technologies, in particular the use and development of safe and secure AI systems, IoT technologies, and cloud computing. The current insecurity of internet platforms and connected technology leave users at high risk of data breaches and direct attacks. Companies must take responsibility for poor security decisions. That is why Access Now has supported efforts like the Paris Call for Trust and Stability in Cyberspace that recognize the responsibility of all actors, including the private sector, in strengthening the security of platforms and services. We believe there is a need to reinforce efforts to improve protections for users and their rights. For example, the Global Commission on the Stability of Cyberspace,[19] a body that works "to promote mutual awareness and understanding among the various cyberspace communities working on issues related to international cybersecurity" has released a package of norms that aim for a more peaceful cyberspace and restraint by states against disrupting core internet infrastructure. Those norms overlap with the commitments of the Paris Call, including the need to address vulnerabilities, the harm of private-sector offensive hacking operations, and the recognition of the value of cyber hygiene.

2. **Developing Norms that Address All Objectives Equally**

   The existing norms should be mapped against the defined objectives. This exercise will help to define potential gaps of the agreed norms. Some norms, for example, concentrate on the protection of state interests and aim to promote stability and security among states by improving the predictability of state behavior. The promotion of peace, stability, and security is an important goal of international norms in the ICT environment. It is, however, important to identify norms that also keep the interests and trust of humans, societies, and businesses in mind. For example, ensuring universal, open, and secure access to the internet globally is key to the realisation of the Sustainable Development Goals (SDG),[20] and the OEWG can help mainstream this thinking, particularly amongst the many States that are not part of the GGE process. It should be on the agenda of the OEWG to examine how improved adoption of the existing commitments and voluntary norms on cybersecurity from UN discussions would protect and facilitate the realisation of the SDGs, particularly as the internet and communication technologies have become so core to societal and economic functioning.

[19] https://cyberstability.org/
[20] https://www.accessnow.org/cant-reach-u-n-goals-sustainable-development-without-internet/

3. **Build a Secure Cyberspace with Humans in Mind**

International norms for a secure ICT environment should not only serve the interests of states; they must aim to ensure the security and integrity of individuals communication. The integrity of ICT systems is not only a concern for states. It is also crucial for sustainable development and the social well-being of humans when they communicate online or make use of new technologies in their daily lives. This focus on the human being and individual centric cybersecurity must be explicitly an objective for the OEWG's deliberations and any reports it publishes.

Additionally, the OEWG should facilitate the participation of the UN human rights system, including Special Procedures and thematic rapporteurs (from the UN and regional human rights bodies) and the OHCHR, as needed. This should be to connect and document the specific cybersecurity related findings and recommendations from these initiatives that have come in their human rights reporting and norm guidance. OEWG discussions must also take on board the specific declarations and norms accepted by the UN Human Rights Council and the General Assembly in its Third Committee resolutions, including on internet freedom (A/HRC/RES/38/7) and the right to privacy in the digital age (A/RES/73/179), and strive to advocate that any further norm development or enforcement around cybersecurity in the context of international peace and security respects these fundamental human rights. That should include understanding existing evidence around targeted disruption of internet communications as well as the human rights value of secure communication systems.

4. **Ensure OEWG discussions engage with the bottom-up, internationally distributed nature of cybersecurity**

Cybersecurity is an everyday, internationally distributed ecosystem, and the OEWG should continue to recognise this. As part of this, we recommend better integration of the OEWG process with regional discussions. As many stakeholders have requested, reports compiled after the regional consultations of the OEWG (currently underway) need to be made public in order to foster debate and integration across all stakeholders. States need to confirm and work with the UN secretariat to ensure this becomes standard practice for all regional consultations and the work plan of the OEWG. Civil society organizations allowed to take part should not be limited to those accredited by the Economic and Social Council, but rather the UN should dedicate resources to ensuring broad representation in the room and participating remotely.

Additionally, we believe it is crucial that the OEWG take further steps to include inputs and participation by a key constituency: security researchers. Security researchers must be empowered to inform the technical discussions taking place through the OEWG. More information security focused initiatives and organisations need to be allowed into the OEWG process. We are concerned that the incident response community and those who work on digital security research and information security strengthening are currently unable to adequately provide their expertise into OEWG deliberations. It is important for the international community and OEWG-engaged states to understand the work that technologists do regarding threat modeling and base OEWG deliberations on their expertise.

V. Conclusion

The first substantive meeting of the OEWG in September has created an environment for a constructive debate to make further progress on international norms in the ICT environment based on existing agreements. To start the discussion on the GGE consensus reports, however, does not mean that some norms require further concretization. Some norms might also need to include more comprehensive consideration in order to achieve a safe, secure, and rights-respecting ICT environment for all.

In this regard, Access Now encourages government representatives to address inter alia the following questions:

- What does the promotion of a safe and secure ICT environment mean? Should this objective include the international security among states, the national security interest of states or the security and integrity of the ICT systems themselves? Where do the human rights of users and interests of at-risk communities fall?
- What objective shall be achieved by the agreed norms? Where is it possible to identify gaps? Which objectives are not sufficiently addressed by the existing voluntary, non-binding norms?
- How will these norms be implemented to adequately prevent and mitigate harms to individuals and societies? What measures might accompany these norms to facilitate action?

This discussion paper was prepared by Nele Achten; with inputs by Raman Jit Singh Chima and Peter Micek.

For More Information, please contact:
Raman Jit Singh Chima | raman@accessnow.org | +1-888-414-0100 x709