UN First Committee Processes on Responsible State Behaviour in Cyberspace: An Explainer

In late 2018, the UN First Committee established two parallel processes to discuss responsible state behaviour in cyberspace – the UN Group of Governmental Experts (GGE) and the Open Ended Working Group (OEWG). The outcomes of these processes may end up having a significant influence on trends and policies in cybersecurity globally, with implications for human rights. This explainer offers human rights defenders all the information they need to start engaging with the GGE and OEWG, from a rundown of the key issues on the GGE and OEWG agendas, to guidance on how the processes work, and when and where human rights defenders can get involved.

What is the UN General Assembly's First Committee and why is it relevant for cybersecurity?

The First Committee is one of the six main committees of the UN General Assembly (UNGA). It's where states address global challenges and threats to peace that affect the international community and seek ways to promote international security and disarmament. Since 1998, when Russia introduced a resolution on "Developments in the field of information and telecommunications in the context of international security", it has been a key forum for the discussion of issues related to state behaviour in cyberspace.

Since then, the UN Secretary General (UNSG) has presented annual reports to the General Assembly on these issues, based on the inputs of member states.

The First Committee has addressed issues related to cybersecurity in primarily two main ways: first, by adopting a resolution on "Developments in the field of information and telecommunications in the context of international security" almost every year since 1998; second, it has also periodically set up a mechanism called a "Group of Governmental Experts" (GGEs).

What has the role of the UN First Committee been so far?

When it comes to cybersecurity-related issues, arguably the most important mechanism of the First Committee has been the GGEs. The first GGE on "Developments in the field of information and telecommunications in the context of international security" was set up in 2004. Through the GGEs, which are set up through the passing of a resolution by UNGA member states, a group of member states selected by the UNSG nominate experts to hold discussions on the issues outlined in the mandate set out by the relevant resolution. If they all agree, the GGE produces a consensus report which is then presented at the General Assembly for endorsement by all member states. The GGEs, of which there have been five on the topic of "Developments in the field of information and telecommunications in the context of international security" since 2004, can be credited with some important achievements towards the advancement of norms, rules, and principles for responsible state behavior in cyberspace. For example, previous GGEs have agreed that the UN Charter and international law (including respect for human rights and fundamental freedoms) apply to cyberspace, and recommended a series of confidence-building measures and voluntary, non-binding norms (see p. 7 of in the 2015 GGE report A/70/174)[1].

The last GGE (2016-2017) was not able to issue a consensus report, apparently due to disagreements around how certain concepts in international law (like the right to self-defence and law of state responsibility, including countermeasures – apply in cyberspace), as well as the question of whether international humanitarian law (which seeks to limit the effects of armed conflict) should apply to cyberspace at all. And although GGE norms have been referred to elsewhere (like at G7[2], the G20[3], and ASEAN[4]), actual implementation of the recommendations included in its reports has been slower.

There are a number of cybersecurity-related issues that the First Committee hasn't dealt with, including technical standards and cybercrime. These are dealt with in other parts of the UN, including its specialised agencies, as well as non-UN forums. For example, the ITU develops technical standards to promote cybersecurity. There are also various processes and initiatives that deal with cybercrime, including within the United Nations Organisation on Drugs and Crime, which oversees an open-ended intergovernmental expert group meeting on cybercrime. However, although the First Committee hasn't dealt with these issues yet that doesn't mean that there haven't been attempts made by some member states for the discussions in the First Committee to be broader in scope when it comes to cybersecurity. In fact, the creation of a parallel process to the GGE, an "Open Ended Working Group" (OEWG) in late 2018 points to an attempt to broaden the scope of discussions. Although both the GGE and OEWG ostensibly have an identical remit (that is, to discuss responsible state behaviour in cyberspace and come up with recommendations) the existence of two parallel processes points to underlying disagreements among states – which is dealt with in more detail below.

What are the key issues on the agenda?

For both the GGE and the OEWG, the resolutions that set them up (see here for the GGE resolution[5], and here for the OEWG resolution[6]) provide the basis for their agendas.

Both the GGE and OEWG will discuss the further development of rules, norms and principles around responsible behaviour of States, possible cooperative measures to address threats, and how international law applies to the use of information and communications technologies.

However, the OEWG resolution also includes text which suggests that the norms that have already been agreed could be amended and a new mechanism created within the UN. Specifically it says, the OEWG may "introduce changes… or elaborate additional rules of behaviour; to study the possibility of establishing regular institutional dialogue with broad participation under the auspices of the United Nations". New issues for the First Committee, were included in the OEWG resolution too, such as "false news or distorted news" and "hostile propaganda", which means that participants of the OEWG are likely to discuss those as well.

Why should human rights defenders care?

In the digital age, a free, open and secure cyberspace is a necessary precondition for the exercise of human rights, online and offline. People increasingly rely on internet infrastructure and connected devices to exercise their rights. If the internet is not secure, human rights can be threatened. For example, weakened encryption and the insertion of backdoors can make it easier for malicious hackers to gain access to personal communications and metadata. In the case of human rights defenders and their networks, the exposure of their data can even put their personal security at risk.

There are four main reasons the discussions at the First Committee on cyberspace should concern human rights defenders:

1. **The promotion of peace and stability in cyberspace is important for human rights**: Recent cyberattacks have resulted in the closure of hospitals, electrical grids and large industries, and even affected the integrity of democratic processes. These incidents – which directly affect the lives of ordinary citizens – show that the discussion of responsible state behaviour is closely linked to human rights. Without understanding and agreement between states on what responsible state behaviour looks like, cyberattacks could continue to undermine democratic institutions and even escalate into conflict. Engaging in these processes can provide an opportunity to promote measures like confidence-building measures (which can help to reduce the risk of escalation), and emphasise approaches that promote the stability and security of cyberspace – like principles of coordination and support for cybersecurity capacity building, as well as measures which promote and protect human rights, including the right to privacy.

2. **Recommendations in the outcomes of the processes could pose risks to human rights**: Just as the recommendations coming out of the GGE and OEWG could promote human rights and a secure and stable cyberspace, it's also possible that they might do the exact opposite – in particular, by promoting measures of state control over information. Over the years, states have proposed measures in the First Committee which would restrict the flow of information online and undermine human rights. For example, the Shanghai Cooperation Organization (SCO), which includes China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan introduced their "International Code of Conduct" in 2011 and 2015, which emphasises state sovereignty and territoriality in the digital space, and suggests a redefinition of the application of international human rights law to give governments greater control over the internet. The resolution that set the OEWG up initially drew on text from the Code, which was removed from the version that was ultimately adopted. Nonetheless, the resolution retained an emphasis on state sovereignty and information control, which could undermine freedom of expression and the free flow of information online.

3. **What happens at the global level influences processes at the regional and national level (and vice versa)**: Global norms can have an important influence on what states do at the national and regional level, and – to be implemented – may even require regulatory instruments and model laws at the national level. At the same time, these processes could be an opportunity to ensure positive developments happening at these levels– like the emphasis on coordination among states and among different stakeholders which are now included in many national and regional cybersecurity strategies – are also reflected at the global level.

4. **It's an opportunity to push back against closing civic space**: There is an increasing tendency to discuss issues related to cyberspace or the internet (especially security-related issues) in closed, government-only spaces, despite the relevance of these discussions to a broad range of stakeholders. Non-government stakeholder engagement in the First Committee processes could therefore set an important example when it comes to stakeholder engagement in cybersecurity-related policy processes at the global level.

How do the First Committee processes connect to other processes and events?

Since the GGE last released a consensus report in 2015, a number of other processes have contributed to the discussions relating to responsible state behaviour in cyberspace, in particular by offering proposals for specific norms that states should adopt. For example, the Global Commission on the Stability of Cyberspace (GCSC), which is made of global cybersecurity experts, has developed two norms for adoption by relevant stakeholders: one on the "protection of the public core", and one on "election infrastructure". It is currently finalising six further norms.

Multilateral forums like the OSCE, NATO, APEC and the BRICS Summit have also contributed to the norm development process by either developing confidence-building measures, updating existing legal guidance (like the Tallinn Manual), or releasing statements following summits (like the BRICS Summit Declarations and NATO Summit Declarations). Adding to this, a number of states have entered bilateral accords, and the EU has adopted a number of resolutions relating to cybersecurity.

As mentioned before, more countries have developed regional and national cybersecurity strategies which indicate their positions on the measures necessary to promote cybersecurity. And a number of private sector initiatives have suggested their own cybersecurity norms: including Microsoft's Tech Accord[7], Siemens's Charter of Trust[8], and Kaspersky Lab's Global Transparency initiative[9]. It is very likely that these developments will inform the GGE and OEWG discussions. Their impact will depend on the engagement of member states and other stakeholders in the processes. The GGE resolution notably requests that the GGE host consultations with regional organisations including the OAS, the AU and ASEAN – which means that discussions happening outside the First Committee will influence the GGE.

What's happened so far at the GGE and OEWG –and what's coming up?

THE GGE

There are only a limited number of spaces for membership of the GGE. UN member states must apply for membership to the UN Secretary General. The UNSG considers applications on a range of criteria such as regional diversity, engagement in previous GGEs and on the relevant issues. This process closed at the end of January 2019, and members were selected in April 2019. From this point on, preparations for the regional consultations (see above) will happen before the first meeting of the GGE from 9-13 December 2019. Tentative dates for the three other GGE meetings have also been set (see below).

Although not publicly confirmed by the UNSG's office at the time of publication, the members of the GGE were notified of the successful outcome of their applications in mid-April and are listed below according to regional grouping:

- Africa: Kenya, Mauritius, Morocco, South Africa
- Asia: China, Japan, Jordan, India, Indonesia, Kazakhstan, Singapore
- Eastern Europe: Estonia, Romania, Russia
- LAC: Brazil, Mexico, Uruguay
- Western Europe and others: Australia, France, Germany, Netherlands, Norway, Switzerland, UK, USA

The GGE resolution also requests that the GGE consult with several regional organisations including the African Union (AU), the European Union (EU), the Organization of American States (OAS), the Organization for Security and Cooperation in Europe (OSCE) and the Regional Forum of the Association of Southeast Asian Nations (ASEAN). Although some organisations haven't announced when their consultations will be yet, others have begun preparations. For example, the OSCE and EU will be having consultations in June, and the OAS will be holding theirs in August. Neither the AU nor ASEAN had confirmed theirs at the time of publication.

THE OEWG

Any member state can register for and attend the OEWG. So far, the dates for the organisational meeting have been set (3-4 June 2019), and the first substantive meeting has been set for 9-13 September. Tentative dates for the rest of the meetings have also been set.

At the OEWG's organisational meeting at the UN headquarters in New York in June, the agenda and modalities for participation, including modalities for consultations with NGOs, will be agreed. The OEWG will then hold three substantive sessions to discuss the issues on its agenda before it is due to present its report to UNGA in October 2020.

TIMELINE FOR GGE AND OEWG

The current dates for the GGE and OEWG sessions, as well as informal consultations, are:

- 3-4 June 2019: Organisational meeting of the OEWG
- 9-13 September: First substantive session of the OEWG
- 2-4 December: Multistakeholder informal consultation for the OEWG
- 5-6 December: Informal consultation of the GGE for non-members of the GGE
- 9-13 December: First session of the GGE
- 10-14 February 2020: Second substantive session of the OEWG
- March 2020: Second GGE session
- July 2020: Final substantive session
- August 2020: Third GGE session
- May 2021: Final GGE session

How to engage

The main actors in both the GGE and the OEWG are member states. Any opportunities for non-government stakeholders to engage will depend on the modalities agreed by member states, informed by the resolutions which set them up and which include guidance on stakeholder engagement. It's therefore important that human rights defenders start engaging now, with a particular focus on influencing the modalities of participation, and encouraging member-states to provide opportunities for meaningful input from non-government stakeholders.

The OEWG resolution includes the possibility of holding two multistakeholder intersessional consultations (that is, sessions held outside its four main sessions) with non-government stakeholders. The first will be held December 2-4 in New York, before the GGE consultations (see the timeline above). These two-day sessions are expected to include opportunities for NGOs to take the floor and make statements on issues relevant to the OEWG's agenda. It is not yet clear how open the modalities will be for the multistakeholder intersessionals. Established practice allows relevant NGOs which are granted access to the UN premises (organisations with consultative status with ECOSOC[10] or accredited to DPI[11]) to register to attend the four main meetings of the OEWG. However, it will be at the June organisational meeting when states decide whether to go with established practice or adopt more permissive or restrictive modalities for NGO participation.

The resolution that set up the GGE doesn't include any mechanisms for engagement with non-governmental stakeholders. However, it is possible that the consultations with regional organisations (see above) may include opportunities for non-governmental stakeholders to engage.

Human rights defenders can also take advantage of various informal advocacy opportunities – including reaching out directly to representatives of member states participating in the processes, and organising side events on the margins of the OEWG and GGE meetings and during the annual First Committee session, which takes place in October. The ability to participate in sessions or organise side events usually relies on having ECOSOC status, and all requests for side events at the UN in NY requires sponsorship either by member state's mission or by departments or offices of the UN. However, opportunities for non ECOSOC accredited NGOs to engage will vary depending on the mechanism. For example, as mentioned, the OEWG could decide to extend the invitation to its meetings to non-ECOSOC accredited NGOs. Non-ECOSOC accredited NGOs can also partner with missions to the UN, departments or offices of the UN and ECOSOC-accredited NGOs to organise side events, and can be accredited for participation in events by ECOSOC-accredited NGOs.

End notes

1. 2015 GGE report A/70/174, https://undocs.org/A/70/174
2. G7 Principles and Actions on Cyber, https://www.mofa.go.jp/files/000160279.pdf
3. 2015 G20 Leaders' Communiqué, http://www.g20.utoronto.ca/2015/151116-communique.html
4. 2nd ASEAN Cyber Norms Workshop, https://ict4peace.org/activities/policy-research/policy-research-cs/2nd-asean-cyber-norms-workshop-in-singapore-supported-by-ict4peace/
5. GGE resolution, https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/266
6. OEWG resolution, https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/27
7. Microsoft Tech Accord, https://cybertechaccord.org/
8. Siemens Charter of Trust, https://new.siemens.com/global/en/company/stories/research-technologies/cybersicherheit-charter-of-trust.html
9. Global Transparency Initiative, https://www.kaspersky.com/about/press-releases/2017_trust-first-kaspersky-lab-launches-its-global-transparency-initiative
10. ECOSOC, https://esango.un.org/civilsociety/displayConsultativeStatusSearch.do?method=search&sessionCheck=false
11. DPI, https://esango.un.org/civilsociety/displayDPISearch.do?method=search&sessionCheck=false

About this explainer

This explainer was authored by Sheetal Kumar of Global Partners Digital and Deborah Brown of the Association for Progressive Communications.