Media Foundation for West Africa

Using the OEWG to open doors and build partnership for a secure and human-centric internet in Africa

with funding support from: GLOBAL PARTNERS DIGITAL

The Media Foundation for West Africa acknowledges the immense contribution of Ms Anriette Esterhuysen in the production of this Policy Brief.

"Everyone has the right to benefit from security, stability and resilience of the Internet. As a universal global public resource, the Internet should be a secure, stable, resilient, reliable and trustworthy network. Different stakeholders should continue to cooperate in order to ensure effectiveness in addressing risks and threats to security and stability of the Internet."
The African Declaration on Internet Rights and Principles.[1]

1 https://africaninternetrights.org/

Table of Contents

What is the Open-Ended Working Group?

The first Open-Ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security is a United Nations-based forum that was established by the UN General Assembly (UNGA) in December 2018.[2] It started its work in June 2019 and presented its final report in March 2021. Its core focus was **responsible state behaviour in cyberspace** – building on the work of previous Groups of Governmental Experts (GGEs). In December 2020 the UNGA agreed on a **second OEWG** that would run from 2021 to 2025. Read more about this new OEWG below.

The first OEWG's scope of work[3]

The OEWG was mandated to examine relevant international concepts aimed at strengthening the security of global information and telecommunications systems and to share views and assessments of the work and recommendations of the GGE particularly with regard to:

- General awareness of information security issues
- Developments in the field of information and telecommunications in the context of international security
- National level efforts to strengthen information security and promote international cooperation
- Measures that could be taken by the international community to strengthen information security at the global level

On the norms and principles of responsible behaviour of States developed by GGEs:

- If necessary, develop these further, introduce changes or elaborate additional rules
- Look at how they can be implemented
- Study the possibility of establishing regular institutional dialogue with broad participation under the auspices of the United Nations
- Continue to study existing and potential threats in the sphere of information security with a view to building common understanding of these threats and explore possible cooperative measures to address them
- Consider confidence-building measures and capacity-building, and, how international law applies to the use of information and communications technologies by States.

The resolution also reaffirmed that States have the right to combat the dissemination of **false or distorted news** that can be interpreted as interference in the internal affairs of other States – or as

2 In late 2018 the UN First Committee – indicative of lack of agreement between member states - established two parallel processes to discuss responsible state behaviour in cyberspace: a new round of the UN Group of Governmental Experts (GGE) as well as an Open Ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security. The UN Office on Disarmament Affairs (UNODA) would be the Secretariat for both the GGE and the OEWG.

3 Adapted from Resolution A/RES/73/27 adopted by the General Assembly on 5 December 2018.

being harmful to cooperation and friendly relations among States. It recognised the duty of a State to abstain from any "defamatory campaign, vilification or hostile propaganda" for the purpose of interfering in the internal affairs of other States.

Participation in the first OEWG

In the UN an "open-ended" working group usually means that all UN Member and Observer States as well as intergovernmental organizations and non-governmental organizations with Economic and Social Council (ECOSOC) consultative status can participate.[4] In fact, the resolution that established the OEWG noted that states would benefit from the participation of the private sector, academia and civil society organizations.

Civil society organisations who had identified cybersecurity as a priority anticipated finally being able to engage openly with UN member states in a global intergovernmental forum and several applied for accreditation. However, no new nongovernmental entities were accredited, and only those with ECOSOC consultative status could observe OEWG sessions. Others were able to participate in a dedicated intersessional meeting with nongovernmental entities convened in December 2019. However, civil society, working closely with the academic and technical community, formed a supportive informal coalition with those who do have ECOSOC status to create the opportunity for others to participate.

To provide for more inclusion, the OEWG accepted written inputs from nongovernmental entities and the December 2019 intersessional was attended by 114 organisations from around the world including from civil society, the private sector and academia. All OEWG sessions were webcast on the UN's online television channel.

4 https://www.ohchr.org/EN/HRbodies/HRC/WGCRC/Pages/OpenendedWorkingGroupSession1.aspx

Overview of participation in the 1st OEWG[5]	
Working papers and proposals submitted	x submitted in 2019 x around 30 submitted by 17 member states – none by an individual African state but a paper on the Programme of Action included endorsement from the following African states: Egypt, Gabon, and Morocco. 6 x informal papers by NGOs 2 x informal papers by IGOs x 12 contributions from NGOs, IGOs and CSOs to the December 2019 Intersessional meeting with nonstate actors – 1 from an individual African entity, Research ICT Africa
Interventions from the floor during interactive discussions in the substantive sessions	First session, 9-13 September 2019: 237 x interventions from 76 member states of which x 20 interventions were from 9 African states of which 2 were expert inputs. African states that made interventions were Algeria, Botswana, Egypt, Ghana, Kenya, Morocco, Mauritius, Nigeria and South Africa. Experts were from Egypt and Kenya. x 1 input from NAM which includes African states. Informal Intersessional, 2-4 December 2019: Around 181[6] interventions of which around x 8 were from x 6 African nongovernmental actors: Cyber Security Experts Association of Nigeria (CSEAN), Paradigm Initiative, Research ICT Africa, KICTANet, Strathmore Law School and AfricaCert. Multiple interventions that included African input from Global Partners Digital, Association for Progressive Communications and Access Now. Egypt was the only African state that made an input. The Cyber Security Experts Association of Nigeria (CSEAN) made scene-setting remarks at the opening and KICTANet presented expert input on cyber-capacity building[7]. Regional intergovernmental organisations from Europe, Asia, the Americas and the Caribbean made multiple interventions. No regional African intergovernmental institutions spoke. Second session, 10-14 February 2020: Out of around 260 interventions from states, 39 were from 12 African states. They were Algeria, Cameroon, Egypt, Ghana, Kenya, South Africa, Malawi, Mauritius, Nigeria, Morocco, Ethiopia and Uganda. Third session, 8-12 March 2021: x 165 contributions from states with x 18 of these from x 8 African states. They were Algeria, Cote d'Ivoire, Egypt, Kenya, Morocco, South Africa and Zimbabwe. Two African nongovernmental organisations made.

5 These numbers are a rough estimate compiled from https://www.un.org/disarmament/open-ended-working-group/ and https://reachingcriticalwill.org/.

6 Note that this is the number of interventions, not the number of states. Several states made more than one intervention.

7 KictaNet's expert input: https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/oewg/statements/4Dec_KICTANET.pdf

Contributions on draft versions of the OEWG report	contributions during the open segments, Research ICT Africa and Consortium d'Appui aux Actions pour la Promotion et le Développement de l'Afrique (CAPDA) x 21 NGO contributed – no individual African NGO or IGO but African NGOs co-drafted and signed several joint CSO contributions. African NGOs that co-signed a contribution on the draft report included Kenya ICT Action Network (KICTANet), Research ICT Africa, Media Foundation for West Africa and YMCA computer training centre and digital studio, the Gambia.[8] x 39 member states made x 86 individual contributions – x 8 from x 4 African states: Egypt[9], Kenya[10], South Africa[11] and Zimbabwe[12].

Timeline and convenings

The OEWG had its first meeting to deal with organisational matters in New York in June 2019 and its third and final substantive meeting in March 2021. It adopted its final report on 12 March and presented it to the 75th session of the UN General Assembly.

Convenings	1 x organisational session – New York, 3-4 June 2019 and 3 x substantive sessions – New York, 9-13 September 2019; New York, 10-14 February 2020 and New York, 8-12 March 2021 and several informal, virtual, sessions.
Meetings with nonstate actors	1 x intersessional meeting with industry partners and NGOs – New York, 2-4 Dec 2019 and 2 x informal multistakeholder segment during the February 2020 and March 2021 meetings

Why is the OEWG important?

The stability and security of the internet is important

As the internet's role in people's economic, social and political lives expands, the more its security and stability matters. Whether we are using the internet for business, banking, to file freedom of information requests, for communicating with colleagues, friends and family, or for reading the news, we need to be able to trust that it is secure, that our communications are not being intercepted or surveilled. The OEWG deals specifically with "international" security – threats and attacks that are linked to conflict, or even tension, between states. Such attacks can have a lot of collateral damage, causing disruption or harm to unintended target countries and individuals thus

8 https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/oewg/documents/comment-joint-ngo.pdf
9 https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/oewg/documents/comment-egypt-zd.pdf
10 https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/oewg/documents/comment-kenya-zd.pdf
11 https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/oewg/documents/comment-southafrica-zd.pdf
12 https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/oewg/documents/comment-zimbabwe-zd.pdf

contributing to internet insecurity and instability more broadly. The impact of cyberthreats and malicious cyber operations impacts people differently, based on their access to power and resources. Gender also matters in international cybersecurity.

Africa is facing real cyberthreats and is not responding adequately

African countries face a growing array of cyberthreats – from attacks on critical infrastructure to espionage and organized crime. Examples are everywhere, from cybersecurity breaches at banks to ransomware attacks targeting key national port and shipping services.[13] Some of these threats link to and can escalate, tensions between countries putting peace and security at risk.

> "In June 2020, the Ethiopian Information Network Security Agency (INSA) thwarted a cyberattack from an Egypt-based actor known as the Cyber_Horus Group. According to INSA, the purpose of the attack was to create significant "economic, psychological, and political pressure on Ethiopia" over the filling of the Nile River's Grand Ethiopian Renaissance Dam (GERD). The GERD was at the time and continues to be a significant source of tension between Ethiopia and Egypt. Though Ethiopian authorities claimed to have averted a broader attack, the Cyber_Horus Group did manage to hack into a dozen or so government webpages, posting messages threatening war if Ethiopia began filling the dam."[14]

The response from African governments has mostly been inadequate. Most African countries do not have up to date national cybersecurity strategies. Even when countries have strategies in place, they "fail to achieve meaningful impact because their plans are missing fundamental components, do not include key stakeholders, and are not adapted to an evolving threat landscape."[15] The OEWG is based in the UN and is open to participation from all member states. It creates an opportunity for African governments to put their concerns and needs on the global agenda. It could drive more effective regional cooperation, more coordinated national responses, and more collaboration with civil society, the media, business and the technical and academic communities.

Cybersecurity is a human rights issue

"People increasingly rely on the availability, integrity and confidentiality of information and its underlying infrastructure to exercise their rights. If states are engaging in internationally malicious acts—and, as a result, making the internet (and the applications and devices dependent on it) less stable and secure—human rights can be threatened."[16] For human rights defenders and free and independent media practitioners an insecure internet does not just make their work difficult, it can put their lives at risk.

13 https://en.wikipedia.org/wiki/Transnet_ransomware_attack
14 From "Africa's Evolving Cyberthreats" by Nate D.F. Allen, Africa Center for Strategic Studies, January 2021 - https://africacenter.org/spotlight/africa-evolving-cyber-threats/
15 From "African Lessons in Cyber Strategy" by Abdul-Hakeem Ajijola and Nate D.F. Allen, Africa Center for Strategic Studies, March 2022 - https://africacenter.org/spotlight/african-lessons-in-cyber-strategy/
16 https://www.gp-digital.org/wp-content/uploads/2019/12/unpacking_gge_cyber-norms.pdf

"While most people are likely to experience some form of cyber insecurity in their lifetime, even people for whom meaningful access to the internet is a challenge, cyber insecurity is not experienced evenly by everyone. Human rights defenders, journalists, and people in positions of marginalisation or vulnerability, because of their religion, ethnicity, sexual orientation or gender identity, for example, can experience particular risk. For example, they are more likely to be targeted by government or lateral surveillance, and the consequences of more broad threats like data breaches or network shutdowns are often more severe for them because of their location within society."[17]

In 2015, the UN GGE on Developments in the Field of Information and Telecommunications in the Context of International Security confirmed that respect for human rights and fundamental freedoms are of central importance and recommended that States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions on the right to privacy in the digital age, to "guarantee full respect for human rights, including the right to freedom of expression."[18] The OEWG built on this and this recognition represents a vital opportunity for African civil society to leverage a global process that recognises the links between human rights and cybersecurity at regional and national levels.

A secure cyberspace depends on the involvement of civil society

"One of the most common problems with security-oriented strategies across Africa is that they are not sufficiently inclusive. The national security establishment by function, training, and doctrine tends to err on the side of collecting and classifying information rather than sharing it. In cybersecurity, however, broad-based trust, transparency, and the sharing of threat information is crucial so that all actors, be they governments, the security sector, private sector organizations, or civil society groups, can detect and address the latest threats. To achieve maximum impact, contributions from a society-wide spectrum of stakeholders are needed in the design, drafting, and implementation of national cybersecurity strategies.
[snip] The need to include and consult civil society in national cybersecurity strategy and policy is no less compelling [than including the private sector]. Civil society plays a crucial role in helping ensure that national cybersecurity strategies are widely read, popularly supported, and hold the government, private sector, and other actors accountable for misconduct."[19]

The OEWG in spite of constraints in how it was operationalised, does represent growing recognition of the need for cybersecurity discussions to include civil society and other nongovernmental actors. For African civil society this matters, because it creates an entry point for more inclusive processes at regional and national level.

17 https://www.apc.org/en/news/why-cybersecurity-human-rights-issue-and-it-time-start-treating-it-one?fbclid=IwAR36y6gdEOavWyhI085mDGJj69Q19C3RP2xY_-f0f5Jij43_0i-ma95y7Ww

18 From clause 13 (e) in the 2015 GGE report to the General Assembly. https://digitallibrary.un.org/record/799853/files/A_70_174-EN.pdf

19 Abdul Hakeem Ajijola, March 2022 - https://africacenter.org/spotlight/african-lessons-in-cyber-strategy/

OEWG outcomes to date

The first OEWG adopted a consensus report13 in March 2021 that reaffirmed previous GGE outcomes but with new reflections and actionable recommendations included.

Threats

Because the OEWG was more inclusive than the GGE it surfaced the extent of concern that many states have about the increase in the militarisation of ICTs and the vast differences in states capacity to respond, either offensively or defensively. Some states are in principle opposed to the use of ICTs for non-peaceful purposes. Some simply lack the resources and capacity. A fear was expressed that states might, rather than using peaceful measures to settle disputes, resort to using ICTs. States also have very different degrees of access to the ICT supply chain – the development and distribution of software, hardware and services – giving those with major ICT developers within their jurisdictions the option of using vulnerabilities in these products and services in their cyber operations. This latter point was stressed by the African group.[20] The use of ICTs to interfere in states' internal affairs by means of targeted information and disinformation operations is also perceived as a growing threat. Other emerging threats noted included partial or complete intentional disruption of internet services (internet shutdowns) and the drive to more use of "autonomous" ICTs through machine learning and artificial intelligence. Lack of clarity of the responsibilities of the private sector was noted as a concern in and of itself. The group recommended that measures to promote responsible State behaviour should remain technology-neutral. Technology constantly evolves. It is the misuse of the technology that matters, not the technologies themselves.

Rules, Norms and Principles for Responsible State Behaviour

Existing GGE norms were reaffirmed and some states proposed the development of new norms but there was no full consensus on which. What they did all agree to was that, states should on a voluntary basis make and measure implementation, and share experience and good practices. Critical infrastructure was discussed and the OEWG recommended that states should not conduct or knowingly support ICT activity that intentionally damages or impairs the use and operation of critical infrastructure.[21]

For civil society, the emphasis on norms implementation is a very positive outcome even if the OEWG did not establish concrete mechanisms for doing so. The Chairs Summary includes useful language from a human-rights perspective in norms guidance that did not make it to the final OEWG report – particularly in the detailed text provided by Canada on the agreed 11 norms. This

20 Paragraph 10 in the African statement on the zero draft of the OEWG report. https://front.un-arm.org/wp-content/uploads/2021/02/AFRICAN-GROUP-STATEMENT-ON-THE-ZERO-DRAFT-OF-THE-OEWG-SUBSTANTIVE-REPORT.pdf

21 Paragraph 31 of the OEWG final report. https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

text reflects input provided by civil society groups.[22] Norms guidance can "help states develop common understandings on a range of important questions: e.g. the precise scope of 'critical infrastructure', and the role of states vis-a-vis other actors in securing ICT supply chains," and provide "concrete guidance on the implementation of norms, which—if implemented in a human-centric and inclusive manner—could meaningfully contribute to a more peaceful and secure cyberspace."[23]

In the African context however much more awareness has to be raised for the guidance on implementing norms for responsible state behaviour in cyberspace to have impact. African states simply do not see their realities reflected in these norms. In a discussion paper submitted to the OEWG, Research ICT Africa pointed out that the limited technical and institutional capacity of African nations makes some of the GGE norms merely theoretical. For example, the norm on state-sanctioned cyberattacks on critical information infrastructure; no attacks have ever emanated from Africa and most African countries generally lack the capacity to initiate such attacks. Similarly, the norm that calls for states to "take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products" and "seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions," is unlikely to resonate with African states as ICT supply chains generally do not originate in Africa.[24] This does not negate the value of these norms and "localising" them can be an effective entry point for inclusive regional processes – an area where civil society can take the initiative. For African civil society, a good starting point will be to examine the norms and focus on those that have the most relevance regionally, and in their national contexts.

A point of concern for African stakeholders is the report's use of the concept of "critical infrastructure" which is fairly loosely defined, and can be interpreted as comprising any infrastructure that a nation-state declares as "critical". This can be used by governments to justify internet shutdowns.

International Law

Global Partners Digital points out that "there is no mention of the different bodies of international law—including international humanitarian law and human rights law and their applicability in cyberspace—that were present in earlier drafts, due to the resistance from some states, including China and Russia."[25] This is disappointing, as the report does recognize the negative implications for human rights that can result from cyberattacks. Here the Chair should be commended because, as with other contentious parts of the text, he included references to the content of the discussions on international law in the Chair's Summary.[26]

22 https://www.gp-digital.org/the-oewgs-consensus-report-key-takeaways/
23 Ibid
24 https://www.un.org/disarmament/wp-content/uploads/2019/12/Discussion-Paper-OEWG-Intersessional-Meeting.pdf
25 https://www.gp-digital.org/the-oewgs-consensus-report-key-takeaways/
26 https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf

Confidence Building Measures is described as comprising a fairly wide range of measures to achieve more transparency, cooperation and stability and being a concrete expression of international cooperation. They are voluntary and can be an area for collaborative action between civil society, states, and other nonstate actors, particularly from the technical community. The report does not reflect civil society proposals to explicitly link CBMs to human rights, nor does it mention the role of civil society – but nor does it exclude it.

Capacity-building

States concluded that capacity-building in relation to State use of ICTs in the context of international security should be guided by agreed principles that can be interpreted as delinking capacity building from specific political agendas. For African states, as indeed for others from the Global South, this is an important step as they often have to 'trade' capacity development resources and opportunities for explicit or implicit political allegiances with capacity-rich states. These principles can help to create a more level playing field for cyber capacity development and it is positive that gender sensitivity, human rights and fundamental freedoms are flagged.

1st OEWG's Capacity-building Principles

Process and Purpose

- Capacity-building should be a sustainable process, comprising specific activities by and for different actors.
- Specific activities should have a clear purpose and be results-focused, while supporting the shared objective of an open, secure, stable, accessible and peaceful ICT environment.
- Capacity-building activities should be evidence-based, politically neutral, transparent, accountable, and without conditions.
- Capacity-building should be undertaken with full respect for the principle of State sovereignty.
- Access to relevant technologies may need to be facilitated.

Partnerships

- Capacity-building should be based on mutual trust, demand-driven, correspond to nationally identified needs and priorities, and be undertaken in full recognition of national ownership.
- Partners in capacity-building participate voluntarily.
- As capacity-building activities should be tailored to specific needs and contexts, all parties are active partners with shared but differentiated responsibilities, including to collaborate in the design, execution and monitoring and evaluation of capacity-building activities.
- The confidentiality of national policies and plans should be protected and respected by all partners.

People

- Capacity-building should respect human rights and fundamental freedoms, be gender-sensitive and inclusive, universal and non-discriminatory.
- The confidentiality of sensitive information should be ensured.[27]

27 From paragraph 56, Open-ended working group on developments in the field of information and telecommunications in the context of international security: Final Substantive Report, March 2021, UNGA - https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

African civil society should take note that the report notes the value of South–South, South–North, triangular, and regionally focused cooperation, and links capacity-building to transforming the digital divide. It emphasises that capacity building should facilitate "genuine involvement of developing countries in relevant discussions and fora and strengthening the resilience of developing countries in the ICT environment."[28]

Regular Institutional Dialogue was a priority for most African states who participated, and in general, for countries from the Global South. Many asked for a permanent mechanism, and some wanted a return to a 'single track' for discussions on international cybersecurity – with reference to the GGE and the OEWG – but even those, including South Africa, were open to compromise and it was agreed to recommend a new OEWG process. The report also refers to the Programme of Action (PoA),[29] a proposal from France and Egypt for a more permanent, regular institutional dialogue to develop a framework for assessing implementation of agreed norms.

Key takeaways for African stakeholders

What are the key takeaways for African stakeholders going forward into the new OEWG, and, more broadly, towards human-centric international and national cybersecurity on the continent?

Reflections on African participation in the 1st OEWG

African states were relatively active in the OEWG through their UN mission staff attending sessions and participation in either African or Non-Aligned Movement group positions and submissions. Up to around 10 African states made inputs from the floor, but, very few individual states followed the process closely. Egypt, Kenya and South Africa were the most consistent. Most significantly, African states did not make an impact as a region. African civil society participated, but only a relatively small number and in spite of the expertise they represent, they also did not contribute region-specific perspectives. African intergovernmental organisations (IGOs) were absent.

Lack of regional strategies and cooperation

The first OEWG process highlighted the lack of regional strategies and cooperation on the continent– not just between different stakeholder groups, but among governments. Linked to this is the fact that pan-African institutions like AfriNIC[30] and AfricaCERT[31] have appeared to not follow the process. The African Union Commission was also not very active, in spite of

28 Ibid paragraph 58.
29 https://front.un-arm.org/wp-content/uploads/2020/12/joint-contribution-PoA-future-of-cyber-discussions-at-the-un-2-2-2020.pdf
30 https://afrinic.net/
31 https://www.africacert.org/

international cybersecurity capacity and infrastructure being one of its priorities, and relatively close involvement in the Global Forum for Cyber Expertise (GCFE). The African Union Commission (AUC) did host the regional consultation of the GGE in 2019 and in doing so did raise awareness of the OEWG, but it appears to have stopped there. But here the onus also lies on the OEWG working modalities. If the process was more explicitly inclusive of international organisations and non-state actors, it would be easier for bodies like the AUC to galvanise the necessary resources to participate at a higher level.

Lack of capacity, and coordination, at national level

For African states the first OEWG was an opportunity that, while not lost entirely, was certainly not adequately utilised. Based on the number of inputs from African states, and in particular, the absence of consistently presenting coordinated regional positions, the region has a long way to go to get to a point where it is not playing catch-up.

The process revealed that while they generally recognise the importance of cybersecurity, very few African states had the capacity, perhaps even the interest, in participating in what has been, to date, the most open UN-based discussion on international cybersecurity. This extends to effective coordination across government departments at national level, as well as liaison between capitals and missions at the UN. This is not a new problem. "Because cybersecurity is a society-wide concern with government-wide responsibilities, it can often be supremely challenging to ensure alignment across sectors. Military services hesitate to take instruction from civilian ministries. Civilian actors, likewise, are reluctant to work under military direction. This dynamic means that the most appropriate coordinating entity is often an independent cybersecurity authority directly answerable to the office of the chief of state."

The OEWG's final report recognises the importance of "open and transparent exchange of views on perceptions of threats and vulnerabilities, responsible behaviour of States and other actors and good practices, thereby ultimately supporting the collective development and implementation of the framework for responsible State behaviour in their use of ICTs." Such exchanges, be it the OEWG itself, or at national and regional level, constitute "confidence-building measures" in their own right:

> "46. Drawing from the lessons and practices shared at the OEWG, States concluded that the prior existence of national and regional mechanisms and structures, as well as the building of adequate resources and capacities, such as national Computer Emergency Response Teams (CERTs), are essential to ensuring that CBMs serve their intended purpose."[32]

32 Paragraphs 46 and 47 from the OEWG's Final Substantive Report, UNGA, March 2021 - https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

Thus, while the process revealed the lack of national and regional coordination and inclusivity, it clearly recommends that these should be prioritised going forward.

More cooperation and a 'dual track' strategy for African CSOs

The OEWG thus far revealed the need for more capacity among African CSOs to participate consistently and to develop a consolidated regional strategy as well as country-specific national strategies. It also revealed how few African CSOs, even among those concerned with digital rights, are aware of the relevance of international cybersecurity – to human rights, but also to sustainable social and economic development. Those African civil society organisations who did follow the process need to be commended for doing so – in spite of resource constraints. Support – both financial and at the level of coordination and strategising – from CSOs from the Global North proved essential to facilitating the involvement of African CSOs. Some of this support also created opportunities for these CSOs to initiate engagement on the OEWG at national level. But this also reveals a degree of dependency among African CSOs which need to be addressed going forward.

It also reveals a tactical gap. While it is strategic for African CSOs to support common international CSO positions on human rights, and a human-centric approach to international cybersecurity, this should not be their only strategic track. They should also aim to develop joint positions with African states and other African stakeholder groups where there is common ground on issues that are specific to the region. This 'dual track' strategy where African CSOs form alliances both globally and regionally will require more resources, but it is much more likely to promote sustainable partnerships between CSOs, government and other stakeholders – particularly the technical cybersecurity sector, nationally and regionally.

The new OEWG - 2021 to 2025

On 31 December 2020 UNGA resolved to establish a new Open-Ended Working Group on security of and in the use of information and communications technologies for the period 2021 to 2025. Its mandate is to study existing and potential threats to information security, possible confidence-building measures and capacity building, further develop rules, norms, and principles of responsible behaviour of states, and discuss ways of implementing them. It also has to explore the establishing of regulator open-ended "institutional dialogue" under the auspices of the UN. The resolution gives the new OEWG the option of establishing thematic subgroups with a view to fulfilling its mandate and facilitating the exchange of views among States on specific issues related to its mandate. As far as nongovernmental actor inclusion the resolution leaves this optional, stating that the new OEWG "may decide to interact, as appropriate, with other interested parties, including businesses, non-governmental organizations and academia".[33]

33 UNGA resolution A/RES/75/240, 31 December 2020 - https://digitallibrary.un.org/record/3896458/files/A_RES_75_240-EN.pdf

OEWG 2021 to 2025 Fact Sheet	
Chair	Amb. Burhan Gafoor (Ambassador and Permanent Representative of Singapore to the United Nations in New York)
Secretariat	UNODA
No of sessions	11 substantive (estimate) sessions from 2021 to 2025 at United Nations Headquarters in New York.
Reports	Annual progress reports – based on consensus A final report to the General Assembly at its 80th session
1st organisational session	1-2 June 2021 - focused on procedure - hybrid
1st substantive session	13-17 December 2021
2nd substantive session	28 March 28 – 1 April 2022 – Refer to the Chair's letter on the programme and stakeholder participation https://documents.unoda.org/wp-content/uploads/2022/03/Letter-from-OEWG-Chair-dated-7-Mar-2022.pdf
3rd substantive session	25-29 July 2022
4th substantive session	6-10 March 2023
5th substantive session	17-21 July 2023
Consultations with nongovernmental stakeholders	24 March 2022 21 July 2022 2 March 2023 and 13 July 2023
Information on how to participate: https://meetings.unoda.org/section/oewg-ict-2021_ngo-information_16382/	

Several African states have participated thus far. Based on a record of contributions (from the floor) they are: Cote d'Ivoire, Djibouti, Egypt, Ethiopia, Kenya, Morocco, Nigeria, South Africa, and Togo. Only one, Egypt, submitted an input document prior to the session. This was a working paper on the Programme of Action.[34]

Modalities for the participation of non-governmental entities have not been finalised. It is expected this will happen during the March 2022 sessions. There is also no final agreement yet on whether thematic sub-groups will be established or not. If they are, it could be a mechanism for including nongovernmental entities in the OEWG's work.

Opportunities for African stakeholders

For African civil society working collaboratively with CSOs from the Global North, there is a clear opportunity to continue their collaboration and advocate for the new OEWG to:

- Maintain and strengthen a human-centric approach to international cybersecurity.

34 https://reachingcriticalwill.org/disarmament-fora/ict/oewg-ii/statements

- Always include human rights impacts in its exploration of cyber threats and efforts to combat them.
- Explore the gender dimensions of international cybersecurity in more depth.
- Focus on implementation of the recommendations in the OEWG of 2019-21 report, including implementation of the agreed GGE framework on responsible state behaviour.
- Building meaningful stakeholder engagement. It will only be known in March 2022 what precisely the modalities for nongovernmental organisations' participation will be, but it is already known that the consultations with the chair will be open to all interested entities, irrespective of whether they have ECOSOC accreditation or not.

For African civil society working regionally – which can also include participation from their global partners - building meaningful stakeholder engagement is not just about what happens in New York. It is first and foremost about more inclusive national and regional processes.

But there are also other opportunities at regional level. Africa states, in collaboration with other stakeholders, should consider exactly how that framework – developed by and for states with far greater cyber capacity than most African states have – applies in the region, and what needs to be done for African states to implement it in a meaningful manner. Follow up on the recommendations on capacity-building and confidence measures also have specific regional dimensions. The OEWG is also not the only cybersecurity-related process that is relevant to African stakeholders. By working collaboratively and more strategically, African actors – from all stakeholder groups – can share resources in following these processes and sharing insights and opportunities.

Other cybersecurity discussions[35]

The Group of Governmental Experts (GGE)

Discussions on cybersecurity inside the United Nations started as long ago as 1998 when the Russian Federation proposed a draft resolution[36] on "Developments in the field of information and telecommunications in the context of international security" to the First Committee, the committee formed by the General Assembly that deals with international security and disarmament. As the internet became more prominent on government agendas, more resolutions followed, and in 2004 the first Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security was convened.[37]Since then there has been five more GGEs and even though the GGE of 2016 to 2017

35 Useful resources for following these processes include https://dig.watch/ provided by the Diplo Foundation, https://reachingcriticalwill.org/ and https://www.gp-digital.org/insight/trust-and-security/ provided y Global Partners Digital.

36 Resolution 53/70 - https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/760/03/PDF/N9976003.pdf?OpenElement

37 For a helpful historical overview of UN cybersecurity processes refer to this animation done by UNIDIR. https://www.youtube.com/watch?v=JbMn_9uzxfk – UNIDIR

failed to agree on a consensus report, over the years they have contributed basic interpretations of how the UN charter (including respect for human rights) and international law applies in the cyber sphere. Building on this they have developed non-binding norms and principles for responsible state behaviour in cyberspace and proposed approaches to using confidence-building measures and capacity-building to help ensure security.[38] The 2012 to 2013 GGE highlighted the importance of national Computer Emergency Response Teams (CERTS). At least one African state participated in each GGE, but there is little evidence of this participation being reflected in national level processes that involved nonstate actors, or that serves to build a nationally coordinated – across state institutions and government departments – follow up.

GGE	GGE members from the African region[39]
2004-2005	Mali; South Africa
2009-2010	South Africa
2012-2013	Egypt
2014-2015	Egypt; Ghana; Kenya
2016-2017	Botswana; Egypt; Kenya; Senegal
2019-2021	Kenya; Mauritius; Morocco; South Africa

African states that have served as members of the GGE between 2004 and 2021

The Ad Hoc Committee (AHC)[40]

First Committee deliberations have focused on international security. Broader, but related issues have been discussed in other UN spaces. For example, the role of technical standards in internet security at the International Telecommunications Union (ITU) and cybercrime by the United Nations Organisation on Drugs and Crime (UNODC). In September 2019 the UNGA resolved to establish an "Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes" with UNODC as its secretariat.30 Three African states are represented on the Ad Hoc Committee, Algeria (which is the chair), Egypt and Nigeria. The AHC's first substantive session – it met in 2021 on organisational matters - took place in New York at the UN from 28 February to 11 March 2022.

The Programme of Action (PoA)

The PoA was proposed by Egypt and France in 2020 as an open platform for follow up and implementation on various cybersecurity initiatives and activities including previously agreed on norms such as the GGE norms. It states as an objective "ending the dual track discussions (GGE/OEWG) and establishing a permanent UN forum to consider the use of ICTs by States in

38 For an easy to access overview of the GGE convenings and their outcomes see Global Partners Digital's information hub on the topic. https://www.gp-digital.org/unga-explainers/

39 https://ict4peace.org/wp-content/uploads/2017/02/CPI-UN-GGE-Members-2004-2017.pdf

40 https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

the context of international security". [41] It was jointly tabled by more than 40 other states, including, from Africa, Gabon and Morocco. This suggestion of establishing a permanent UN forum to consider cybersecurity has also been made, repeatedly by African states, in the GGE and in the OEWG.

Multistakeholder discussions

After the failure of the GGE to produce a consensus report in 2017, it felt for a while as if United Nations-based processes dealing with cybersecurity had come to a halt. But outside of the UN, cybersecurity discussions gained momentum in "multistakeholder" processes such as the "London Process"[42] and the Freedom Online Coalition (FOC) working group on a free and secure internet.[43] The Global Commission on the Stability of Cyberspace (GCSC) made up of members from all stakeholder groups started its work on norms in 2017. Private-sector initiatives also gained momentum, in particular, the Microsoft-led proposals for a "Digital Geneva Convention"[44] first made in 2014 and Cybersecurity Tech Accord, launched in 2018.[45] Emerging from the London process, the **Global Forum on Cyber Expertise (GCFE)**, continues and has a strong African focus.

Global Forum on Cyber Expertise (GCFE)[46]

Currently, the GFCE is a multi-stakeholder community of more than 140 members and partners from around the world and it has been active in Africa, convening a series of capacity building events in Accra in March 2022. It aims to strengthen cyber capacity and expertise and plays an information clearing house function.

The Global Commission on the Stability of Cyberspace (GCSC)[47]

Established in 2017, the GCSC proposed non-binding norms for both state and non-state actors including a norm on "non-interference with the public-core of the internet".[48] Two Commissioners from Africa and the Commission's final report developed a framework for approaching cyber stability that could be useful to African civil society as they engage with African states and other non-state actors: "This framework includes (1) multistakeholder engagement; (2) cyber stability principles; (3) the development and implementation of voluntary norms; (4)

41 https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-future-of-cyber-discussions-at-un-10-08-2020.pdf
42 The London Process, also known as the Global Conference on Cyberspace or GCCS was a series of international conferences that started in London in 2011 with participants from government, the private sector and civil society focused on practical cooperation on norms and capacity building for responsible behavior in cyberspace. https://en.wikipedia.org/wiki/London_Process
43 The FOC is a coalition of governments who have declared commitment to "online freedom". Non-state actors are included in FOC working groups. https://freedomonlinecoalition.com/blog/wg-1-an-internet-free-and-secure/
44 https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVroA
45 The accord is made up of more than 150 companies committed to protecting cyberspace and its users. https://cybertechaccord.org/
46 https://thegfce.org/
47 https://cyberstability.org/
48 https://cyberstability.org/news/statement-on-the-interpretation-of-the-norm-on-non-interference-with-the-public-core/

adherence to international law; (5) confidence-building measures; (6) capacity building; and (7) the open promulgation and widespread use of technical standards that ensure cyberspace is resilient."[49]

African cybersecurity processes

African states felt increasingly under pressure and under-prepared for dealing with cyber threats – technically and at the level of policy and regulation. In many countries this pressure can be attributed not just to the fear of cyber attacks and the need to address cybercrime, but also to governments' fear of the consequences of the internet being widely used by the media and civil society, and the broader public, as a platform for holding states accountable.

The most comprehensive intergovernmental process has been the African Union Convention on Cyber Security and Personal Data Protection – known as the Malabo Convention – drafted in 2011 and adopted in 2014 to establish a framework for secure electronic transactions, combating cybercrime, the protection of personal data, and the promotion of cyber security and e-governance. The African Union Commission put much effort to involving as many AU member states as possible, and many did participate. However, to date, the Convention has only been signed by eight of the African Union's 55 member states, and ratified – through building national legal instruments that reflect the provisions in the Convention - by one[50]. However, even though the future of the Convention seemed uncertain – 15 member states need to ratify it for it to be enforced – it raised awareness and contributed to cybersecurity capacity development. Very significantly, it made African civil society organisations aware of the risks that cybersecurity legislation can pose to human rights. The 2013 African Internet Governance Forum, held in Nairobi, recommended – endorsed by all stakeholder groups – that with regard to "Security: Legal and other Frameworks – Spam, Hacking and Cyber-crime" it was necessary to "Identify aspects of policies that need to be changed to make legislation more supportive of online freedoms" and to raise awareness and spur multi-stakeholder conversations on "the importance of protecting internet rights the way human rights have always been protected and promoted". On "Openness: Human rights, freedom of expression and free flow of information on the Internet" it was recommended to "Uphold fundamental Human Rights and their principles in the development of national and regional Internet policies", including cybersecurity and cybercrime policies.[51]

At national level many states were fast tracking the development of cybersecurity legislation, often without much consultation with non-state actors and following a broad-brush stroke approach with vague definitions of concepts, posing serious risks for human rights online – particularly the right to freedom of expression and opinion and the right to freedom of assembly. For civil society organisations working on human rights online in Africa who were already facing a full plate of challenges having to also take cybersecurity on board felt like a bridge too far, but nevertheless,

49 https://cyberstability.org/report/#3-the-gcsc-cyberstability-framework

50 https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf

51 From the outcome report and recommendations of the African Internet Governance Forum, Nairobi, 2013. https://www.afigf.africa/sites/default/files/report%20afigf%202013.pdf

they consciously engaged these processes, and in several countries their efforts contributed to preventing excessive harms to human rights in emerging cybersecurity laws.[52]

Conclusion and recommendations for African stakeholders

Cybersecurity – including international cybersecurity that touches on the relationships between states and the responsibility of states linked to international law, including international human rights law - the core of the OEWG's mandate – is important to everyone who cares about the internet or who uses the internet. It is also an area of common interest between different stakeholder groups and can therefore strengthen cooperation between people and institutions that do not always work together; namely civil society, government, business, technical, academic and organisations.

Capacity development and confidence-building measures is a very feasible entry point for African engagement on follow up on the first OEWG and participation in the second. Based on the inputs from interviews with people from all these sectors, this brief proposes the following recommendations:

Civil society organisations should:

- **Raise awareness that cybersecurity AND cybercrime are not niche issues** but core to securing an internet that enables human rights and people-centered development.
- **Broaden the number and range of civil society actors involved**, reaching out in particular to media organisations and CSOs dealing with peace and security and talk to them about cyber norms.
- **Proactively outreach to government nationally.** Find out which government agency is leading in the conversations in their country, and ask to be part of the conversation. Identify capacity-development opportunities.
- **Catalyse national engagement.** If there is no national conversation on cyber norms yet, led by government, civil society can start it, inviting government, businesses, technical and academic institutions. Document national positions. Even informal papers can be influential.
- **Catalyse regional engagement.** Reach out to regional institutions like the African Union, the African Commission on Human and Peoples' Rights (e.g. by convening side events on the OEWG) and strive to have collective African civil society inputs into the OEWG. It is not necessary to build new coalitions. Every existing coalition can focus on OEWG matters and collaborate with others.
- **Be prepared and work collaboratively.** Read all relevant documents including inputs from states around the world. Do this collaboratively and build coalitions across the region.

52 To mention just a few examples, the cases of Kenya, South Africa and Zimbabwe are described in this article by Privacy International dating back to 2018. Since then https://privacyinternational.org/news-analysis/2160/lone-voices-leading-way-how-civil-society-africa-successfully-countering.

Prepare policy positions (in coordination with other partners) which can then be passed to the government delegations.

- **Prepare for participation in every OEWG session.** African civil society should not rely only on international organisations to facilitate their inputs and positions. The role that Global Partners Digital played during the first OEWG was extremely helpful in terms of consolidating civil society inputs. A more African-focused approach led by African CSOs would be even more effective.
- **Do research.** Assumptions are often made that African states assume positions in global forums that are linked to their financial relationships and political allegiances with super powers like China, the Russian Federation, European states, or the United States. But there is very little actual evidence of how this is playing out. Civil society can play a role in gathering evidence and facilitating more transparency.
- **Find common ground with other nonstate actors.** Collaborate with people and organisations from the private sector and the technical community. Reach out to IXPs, data centres, ccTLD (country code top level domain name associations), internet service providers and mobile operators. Talk to companies that already follow the process closely, like Microsoft. Find out who the cybersecurity professionals are in your country and try to include them in opening up the conversation at national level.
- **Be more strategic in leveraging global engagement.** Consider which of the OEWG outcomes and new OEWG conversations can be leveraged to have influence at national level, and, also to link both to opportunities at regional level.
- **Have a holistic approach that includes capacity development, economic and social development, Global South influence and human rights.** Only using human rights as an entry point might not be the best way of building strong national and regional engagement in international cybersecurity.

African states should, at national level:

- **Take the process seriously and follow it.** Even if they cannot attend meetings, they can make written inputs. UN is the only place that provides a forum for them to contribute. The OEWG is an opportunity for African states to have their voice heard and have their recommendations reflected in the final outcome.
- **Approach cybersecurity as a broader social and economic development concern.** They should take on board OEWG recognition of the links between of human rights and international cybersecurity. Many are more focused on cybercrime and developing cybercrime legislation, or using cybercrime and cybersecurity to establish authoritarian measures that impacts negatively on the internet's role in enabling human rights.
- **Actively engage with non-state actors in their OEWG engagement**, from the point of preparatory national engagement prior to OEWG meeting to including them in their delegations, to organising debriefs after each substantive session. The value of doing so lies not in simply supporting the multistakeholder approach, it is, first and foremost, a way of strengthening a country's voice at global level.

- **Make national cybersecurity process more inclusive, open and transparent**. In doing so they have to – in particular – be sure to include civil society. In some countries government agencies work with the technical community and the private sector on national cybersecurity. But they tend to actively excluded civil society, particularly rights advocates.

African states and African IGOs should work regionally to:

- **Make capacity within the AUC a priority.** Without adequate regional facilitation of coordination it will be very difficult for African participation to be more effective.
- **Encourage individual countries to take the lead in facilitating regional coordination.** In the absence of the AUC taking a lead, this could make a huge difference – even if it only starts with small groups of like-minded countries, or sub-regional groups.
- **Convene to discuss outcomes of the first OEWG** (and of the GGE) and their participation and inputs during the second OEWG. The priority should not be to agree on everything, a diversity of views can be healthy but they still coordinate their inputs and share experiences.
- **Share resources to follow all cybersecurity discussions.** They can agree on a division of labour based on where their interest and competencies lie and coordinate their positions regionally, facilitated by, ideally, the AUC.

UNODA and the OEWG chairs should:

- **Provide easy to access information about how non-state actors can participate.** Outreach to IGOs on how they can be involved would be extremely helpful. Assumptions that they know how they can participate, and when, are often wrong.
- **Provide for easier and more effective civil society participation** and recognise the particular value that civil society perspectives will add to the process.
- **Urge member states to make their participation more inclusive**. They can, for example, use templates for seeking inputs that actively encourages member states to reflect perspectives from other stakeholder groups. They can also remind them that they can make their delegations multistakeholder.
- **Transcribe all oral statements.** Not all Global South states submit their oral inputs in writing. Transcription can be automated and it can help build more regional collaboration and contribute to civil society finding common ground with member states.

1st OEWG in numbers and dates	
How/when established?	By UNGA resolution – proposed by Russia - on 5 December 2018
1st OEWG term	2019 to 2021
Chair and Secretariat	Ambassador Jürg Lauber of Switzerland and the United Nations Office Secretariat for Disarmament Affairs (UNODA)
Member state participation	More than 100 UN member states participated with around 20 countries from Africa participating - as in attending - over the course of the OEWG.
Non-state actor participation	Entities with ECOSOC consultative status could observe all substantive sessions. More than 100 NGOs participated in the multistakeholder intersessional in December 2019.
Convenings	1 x organisational session – New York, 3-4 June 2019 and 3 x substantive sessions – New York, 9-13 September 2019; New York, 10-14 February 2020 and New York, 8-12 March 2021 and several informal, virtual, sessions.
Meetings with nonstate actors	1 x intersessional meeting with industry partners and NGOs – New York, 2-4 Dec 2019 and 1 x informal multistakeholder segment during the February 2020 meeting
Documents produced by the Chair and the Secretariat	x 60+ reports, notes, letters, compendiums of submissions and agendas

Media Foundation for West Africa
32 Otele Avenue, East Legon,
Telephone: +233 (0) 302 555 327
Twitter: @TheMFWA
Facebook: Media Foundation for West Africa
info@mfwa.org
www.mfwa.org


@themfwa


www.mfwa.org


themfwa