Our input to the OEWG intersessional

GLOBAL PARTNERS DIGITAL

December 2019

About Global Partners Digital

The advent of the internet – and the wider digital environment – has enabled new forms of free expression, organisation and association, provided unprecedented access to information and ideas, and catalysed rapid economic and social development. It has also facilitated new forms of repression and violation of human rights, and intensified existing inequalities.

Global Partners Digital (GPD) is a social purpose company dedicated to fostering a digital environment underpinned by human rights and democratic values. We do this by making policy spaces and processes more open, inclusive and transparent, and by facilitating strategic, informed and coordinated engagement in these processes by public interest actors.

Our submission

With this input, GPD aims to inform the discussions and shape the outcomes of the Open-Ended Working Group's report. We look forward to exploring further, in concert with all other stakeholders, a common understanding of key concepts and measures to operationalise them. Our input is structured to reflect the mandate of the OEWG, focusing on the following areas: existing and potential threats in the sphere of international security; how international law applies to the use of ICTs by states; confidence-building measures; capacity building measures; rules, norms and principles of responsible behaviour of states.

Central to our input are two key points: 1) discussions relating to peace and security in cyberspace, and what is permissible and impermissible behaviour in cyberspace, are directly tied to and impact human rights 2) due to the characteristics of ICTs as primarily civilian technologies, which were developed and continue to evolve due to the critical involvement of non-state actors, the maintenance of international peace and security in cyberspace must be an effort inclusive of all stakeholders.

We therefore believe there is a need to highlight the implications of the OEWG mandate from a human rights perspective and move the discussion on roles and responsibilities forward. Therefore, with regards to "emerging and existing threats in cyberspace" we provide insight on how these discussions should be approached from a human rights perspective. With regards to the "capacity building" "norms, rules and principles", and "confidence-building measures" we both outline the relationship between these elements of the responsible state behaviour framework and highlight the role of civil society in implementing them. With regards to "the application of international law in cyberspace" and "regular institutional dialogue under the auspices of the UN", we look forward to shaping the discussions together and bringing a human rights perspective.

Existing and emerging threats in cyberspace

Key message: *The way threats are defined shapes responses, and this is why threats in cyberspace should be understood in a way that is focused on protecting the individual, and promoting a human-centric understanding of the development and use of ICTs. Civil society has an important role in supporting governments and other stakeholders to understand the nature of threats in cyberspace.*

Recommendation: *The OEWG should recognise the importance of a human-centric and human-rights respecting approach to both defining and addressing threats in cyberspace.*

Most threats in cyberspace are to civilians in peacetime. Due to the increasing dependence of individuals and societies on ICTs, a human-centric approach to ensuring a peaceful and secure cyberspace therefore supports measures which do not undermine, but rather which support the security and stability of the internet and digital technologies. This includes measures which strengthen the security of the physical infrastructure that supports the internet and the hardware as well as software of digital devices so that everyone can enjoy a secure internet, regardless of their location. Addressing threats emanating from both state and non-state actors must be done in a human rights-respecting manner.

Norms, rules and principles

Key message: *Each of the 11 norms listed in paragraph 1 of General Assembly resolution 73/271 has a link with human rights. In particular, the implementation of each norm can result in a negative or beneficial impact on human rights. Civil society has an important role to play in shaping and implementing the norms and thereby in supporting state actors in their responsibility to promote a secure and stable cyberspace.*

Recommendation: *The OEWG should recognise the important role of all stakeholders, including civil society, in implementing the 11 norms. During forthcoming meetings of the OEWG, states should be encouraged to share their experiences and challenges in implementing the norms. Furthermore, it should recognise the importance of accountability in ensuring operationalisation of the norms. Therefore, going forward, the OEWG should recommend instituting a reporting process that provides periodic and publicly available assessments of states adherence to the norms.*

No changes should be introduced to the rules, norms and principles of responsible behaviour of states as listed in paragraph 1 of General Assembly resolution 73/27, which have already been adopted by consensus by the General Assembly.

We urge the implementation of the existing 11 norms in an inclusive and transparent manner by all relevant stakeholders, including civil society, academia and the private sector. Further, there is a need to recognise the challenges in implementing the norms. This includes the

[1] https://undocs.org/A/RES/73/27

importance of adequate capacity to implement the norms and the need to monitor the norms and state behaviour. Civil society has a role to play in addressing both of these challenges[2].

Regarding norm (a), this norm calls on states to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security. Some of these practices include network disruptions, arbitrary surveillance, censorship, and cyberattacks on human rights defenders. These practices have been widely documented in research carried out by civil society organisations, with recommendations provided on how to address these practices[3].

Regarding norm (b), which relates to the attribution of ICT incidents, it is important to work with all stakeholders to understand the larger context of an ICT incident, including its impact on the enjoyment of human rights. A lack of attribution, or misattribution can lead to the escalation of tensions between states which harms human rights by leading to attacks which compromise access to essential services and the integrity of data. Civil society organisations can bring the perspectives and voices of otherwise underrepresented and vulnerable communities who are disproportionately affected by cyberattacks, as well as provide information on the impact of cyberattacks on the enjoyment of human rights.

Regarding norm (c), which states that "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;" international human rights law states must protect against human rights abuses within their territory and/or jurisdiction by third parties, including business enterprises. Human rights defenders play a role in supporting state's due diligence obligations by monitoring and reporting these abuses and thereby help support state actors to hold private actors to account[4].

Regarding norm (d), it is essential that states efforts to address terrorist and criminal use of ICTs are human-rights respecting. Yet, as documented by the UN Special Rapporteur on "the promotion and protection of human rights and fundamental freedoms while countering terrorism" the restriction of rights and closing of civic space as part of measures to address criminal and terrorist use of ICTs represents an increasing trend[5]. Civil society groups have already played an important role in monitoring these practices, as well as in providing concrete guidance on how states can cooperate to address criminal and terrorist use of ICTs while protecting human rights[6].

---

[2] The text and examples included in this section also appear in a forthcoming publication "Unpacking the GGE's framework on responsible state behaviour: norms", authored by Deborah Brown and Anriette Esterhuysen (Association of Progressive Communications) and Sheetal Kumar (Global Partners Digital).

[3] "Freedom on the Net", Freedom House, https://freedomhouse.org/report-types/freedom-net; Association for Progressive Communications, https://www.apc.org/en/publications; Access Now, https://www.accessnow.org/the-state-of-internet-shutdowns-in-2018/; Open Observatory of Network Interference, https://ooni.org/; "Digital Rights in Africa", Paradigm Initiative, http://paradigmhq.org/download/digital-rights-in-africa-report-2018/; CIPESA, "State of Internet Freedom in Africa 2019", https://cipesa.org/resources/

[4] Amnesty International, https://www.amnesty.org/en/latest/research/2019/10/morocco-human-rights-defenders-targeted-with-nso-groups-spyware/; Citizen Lab, https://citizenlab.org/2017/06/reckless-exploit-mexico-nso/

[5] "Impact of measures to address terrorism and violent extremism on civic space and the rights of civil society actors and human rights defenders - Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism", https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/40/52

[6] "UPR reports", Front Line: International Foundation for the Protection of Human Rights Defenders, https://www.frontlinedefenders.org/en/upr-reports; "Global Statement on the 20th Anniversary of the UN Declaration on Human Rights Defenders" by CIVICUS: World Alliance for Citizen Participation, https://www.civicus.org/index.php/media-resources/news/3717-global-statement-on-the-20th-anniversary-of-the-un-declaration-on-human-rights-defenders-2; "Terrorism/Counterterrorism", Human Rights Watch, https://www.hrw.org/topic/terrorism-counterterrorism; Amnesty International,

Regarding norm (e), which reiterates the importance of upholding human rights in cyberspace, human rights defenders play a wide range of roles. This includes shaping policies, building the capacity of stakeholders to implement frameworks for the national context in a rights respecting manner, providing technical and policy solutions to existing challenges, and raising awareness of existing initiatives and commitments. In addition, they monitor state practice at the national level, conduct research and litigation, and use mechanisms at the regional[7] and global level, in particular the UN Human Rights Council, the Special Procedure system, the Treaty Body system, the Universal Periodic Review (UPR) and the Office of the High Commissioner for Human Rights (OHCHR), to highlight both good practice and violations of human rights. The research and advocacy work conducted by civil society in this regard is crucial in providing the evidence base that promotes compliance with the human rights commitments referred to in this norm.[8]

Furthermore, it is important to recognise that due to the dependence of individuals and societies on ICTs in the digital age, measures which increase stability and security in the use of ICTs are equally critical for the enjoyment of human rights. Therefore, measures which weaken security, such as measures which introduce vulnerabilities or backdoors into software and hardware, both undermine human rights and weaken the security and stability of cyberspace. The importance of technical solutions to secure and protect the confidentiality of digital communications, including measures for encryption and anonymity and human rights have been widely researched and documented by civil society[9].

Regarding norms (f), (g) and (h), critical infrastructure - such as transport, water and wastewater systems, food and agriculture, electricity, financial services and telecommunications - is critical for the enjoyment of a wide range of human rights, including the rights to health, work and education. Resolution 58/199 refers to eleven measures that can be taken, including the promotion of "partnerships among stakeholders, both public and private, to share and analyse critical infrastructure information" and the training and exercises to enhance response capabilities and to test continuity and contingency plans in the event of an information infrastructure attack, and encourage stakeholders to engage in similar activities."[10] Civil society groups currently carry out simulation exercises and training[11], as well as promote national and international research, and promote the application of security technologies that meet international standards[12].

Regarding norm (i) confidence in the security of ICT products is critical for the exercise of a range of human rights including the rights to freedom of expression, the right to privacy and other civil and political rights, and a range of economic, cultural and social rights, including the

---

https://www.amnesty.eu/news/category/statements-and-reports/human-rights-and-counter-terrorism-statements-and-reports/

[7] http://www.oas.org/en/iachr/expression/reports/annual.asp

[8] APC's Internet Rights programme and the Universal Periodic Review, https://www.apc.org/en/project/universal-periodic-review

[9] "Travel Guide to the Digital World: Encryption policy for human rights defenders", Global Partners Digital, https://www.gp-digital.org/publication/travel-guide-to-the-digital-world-4-encryption-policy-for-human-rights-defenders/; "Defending the right to privacy globally: 8 key recommendations for the digital age", Access Now; https://www.accessnow.org/defending-the-right-to-privacy-globally-8-key-recommendations-for-the-digital-age/ "Encryption", Internet Society, https://www.internetsociety.org/issues/encryption/

[10] A/RES/58/199, https://undocs.org/A/RES/58/199

[11] Chatham House, https://www.chathamhouse.org/publication/annual-review-2017-18; DiploFoundation, https://www.diplomacy.edu/cybersecurity;

[12] Internet Society, https://www.internetsociety.org/resources/

right to work, to health. Ensuring the integrity of the supply chain requires that states refrain from mandating backdoor access to ICT products and messaging platforms as well as preventing the proliferation of malicious ICTs and techniques, through for example malware and software vulnerabilities.

Human rights organisations have already played a role by highlighting the proliferation of malicious ICTs and techniques,[13] in defending human rights in supply chains by developing tools such as 'human rights impact assessments' and in monitoring compliance with human rights standards[14]. They have also recently developed a tool for assessing human rights impact of internet registries[15].

Regarding norm (j) vulnerabilities have been used to attack critical infrastructure, with extremely damaging effects. Good practices relating to vulnerability disclosure include protecting security researchers and clearly outlining the roles and responsibilities of all stakeholders, including vendors, in reporting processes[16]. Civil society have a role to play in ensuring that processes for responsible state disclosure exist, that they do not criminalise security researchers, and that they are inline with best practice.

Regarding norm (k), computer incident response teams represent a wide range of organisations, including non-government actors. The network "FIRST" for example, includes as part of its membership, civil society organisations who provide incident response support for vulnerable populations.[17] The network "Computer Incident Response Center for Civil Society", or CiviCERT, is a network of CERTs, Rapid Response teams, and independent Internet Content and Service Providers focused on supporting civil society to prevent and address digital security issues.[18] In addition, civil society have a role to play in ensuring the establishment and operation of computer incident response teams in a manner that is independent and transparent. This is important from a rights perspective to ensure that a computer incident response team carries out its work without impinging on freedom of expression or privacy.[19]

Capacity building

Key message: *Capacity building efforts have an impact on human rights and need to be tailored and sustainable. Civil society has a role to play in supporting a wide range of capacity building efforts.*

Recommendation: *The OEWG should recognise the role of all stakeholders, including civil society, in both the development and implementation of capacity building efforts. It should also recognise*

---

[13] Reckless VI, Citizen Lab, https://citizenlab.ca/2018/11/mexican-journalists-investigating-cartels-targeted-nso-spyware-following-assassination-colleague/

[14] Business and Human Rights Resource centre, https://www.business-humanrights.org/

[15] "Assessing the human rights impacts of Internet registries", Article 19, https://www.article19.org/resources/assessing-human-rights-impacts-internet-registries/

[16] Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges, CEPS, https://www.ceps.eu/ceps-publications/software-vulnerability-disclosure-europe-technology-policies-and-legal-challenges/

[17] https://www.first.org/members/map

[18] https://www.civicert.org/

[19] National CSIRTs and Their Role in Computer Security Incident Response, New America Foundation, https://www.newamerica.org/cybersecurity-initiative/policy-papers/national-csirts-and-their-role-in-computer-security-incident-response/

the importance of the need for tailored and sustainable capacity building efforts. The OEWG should take stock of existing capacity building efforts and requirements to determine issues and topics where further capacity-building expertise and processes may be necessary, while identifying possible duplications of effort.

In order to be holistic and effective, capacity building should be understood to encompass a wide range of efforts, including the development of cybersecurity policy, cyber incident management and critical infrastructure protection, cybercrime, cybersecurity culture and skills and cybersecurity standards. Each of these areas links with human rights and includes roles for civil society.

- **Cybersecurity policy**: Both national legislation and international policy discussions and outcomes provide opportunities to promote a human-centric and human-rights respecting approach to global cybersecurity issues. At the national level, for example, civil society organisations have supported the development of national cybersecurity strategies and inputted into the drafting of relevant legislation[20]. They have also been part of a wide range of multistakeholder efforts to provide guidance on how to develop national cybersecurity policies[21]. Examples of international policy capacity building include the development of toolkits, explainers, tools, and cyber diplomacy trainings to enable stakeholders to participate in cybersecurity discussions at the international level[22].
- **Cyber incident management and critical infrastructure protection**: civil society and multistakeholder initiatives have so far played an important role in providing guidance on how to set up CSIRTs and manage cyber incidents[23].
- **Law Enforcement Capacity Building:** the development and enforcement of legislation, law enforcement capacity, and cross-border cooperation is required to ensure that individuals are protected from crime. Each of these elements can impact on human rights. For example, the definition of what constitutes criminal activity has strong implications on human rights. Training subsequently has direct impacts on the enforcement and legal interpretations of the legislation as well and rights such as the right to effective remedy. Civil society organisations have provided guidance on how ensure cross-border cooperation to address crime while respecting human rights[24].

---

[20] Multistakeholder Approaches to National Cybersecurity Strategy Development, Global Partners Digital, https://www.gp-digital.org/publication/multistakeholder-approaches-to-national-cybersecurity-strategy-development/

[21] "Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies", Organisation for Economic Co-operation and Development (OECD), https://www.oecd.org/sti/ieconomy/comparativeanalysisofnationalcybersecuritystrategies.htm; "Guide to developing a national cybersecurity strategy - Strategic engagement in cybersecurity, International Telecommunications Union", https://www.itu.int/pub/D-STR-CYB_GUIDE.01-2018;

[22] UNGA First Committee Info Hub, Global Partners Digital, https://www.gp-digital.org/event/unga-first-committee-hub/, Global Forum on Cyber Expertise, https://www.thegfce.com/

[23] "Establishing and supporting Computer Incident Security Response Teams (CSIRTs) for Internet security" Internet Governance Forum (IGF) Best Practice Forum on Cybersecurity https://intgovforum.org/multilingual/content/establishing-and-supporting-computer-incident-security-response-teams-csirts-for-internet; "Global Good Practices - National Computer Security Incident Response Teams (CSIRTs)" GFCE, https://www.thegfce.com/documents/publications/2017/11/21/national-computer-security-incident-response-teams-csirts; CERT.br, https://www.cgi.br/publicacao/internet-governance-in-brazil-a-multistakeholder-approach/

[24] "How to fix MLATs — and a path toward resolving jurisdictional issues", Access Now, https://www.accessnow.org/fix-mlats-path-toward-resolving-jurisdictional-issues/ ; "Building law enforcement capacity to tackle cyber threats: Lessons from year one of capacity building workshops", Observer Research

- **Cybersecurity culture and skills:** organisational policies and public awareness campaigns are key to ensuring a human-rights respecting cyberspace, because—without digital security awareness—users put themselves and others at risk. Awareness campaigns themselves should be human rights-respecting, and should not be used to restrict the use of the internet to access information—for example by discouraging the use of the internet for accessing information about sexual health or other sensitive topics. Many civil society groups provide digital security training, including for vulnerable and at-risk groups[25].
- **Cybersecurity standards**: this includes the development of standards, which can promote human rights[26] and also the delivery of technical assistance in implementing technical standards[27], which can take the form of hands-on training and technical assistance delivered by civil society organisations.

Confidence building measures

Key message: *Confidence-building measures (CBMs) have a link with human rights, and civil society has an important role to play in supporting the implementation of CBMs. Furthermore, open, inclusive and transparent discussions build trust and confidence and are therefore in and of themselves CBMs.*

Recommendation: *The OEWG should recognise the role of all stakeholders, including civil society, in both the development and implementation of confidence-building measures. Further, it should encourage states to share their experience in implementing confidence building measures during the forthcoming meetings of the OEWG.*

Confidence building measures have an important role to play in reducing tension and building trust and confidence between states. This is important from a human rights perspective because insecurity and uncertainty can lead to increased cyberattacks. A lack of trust between states also fuels the securitisation of policy, justifying measures that lead to restrictions on privacy, freedom of expression in the name of protecting national security from attack by other states.

Foundation, https://www.orfonline.org/research/building-law-enforcement-capacity-to-tackle-cyber-threats-lessons-from-year-one-of-capacity-building-workshops/; Joint Civil Society Response to Discussion Guide on a 2nd Additional Protocol to the Budapest Convention on Cybercrime. T-CY (2018)16, https://edri.org › globalcoalition-civilsocietyresponse_coe-t-cy_20180628; "Analysis of the Budapest Cybercrime Convention in the Paraguayan criminal system", TEDIC, https://www.tedic.org/en/analysis-of-the-budapest-cybercrime-convention-in-the-paraguayan-criminal-system/

[25] Colnodo, https://civictech.guide/listing/colnodo/; eQualitie, https://equalit.ie; Tactical Tech,https://tacticaltech.org/#/; Access Now, https://www.accessnow.org/help/; Front Line Defenders, https://www.frontlinedefenders.org/en/digital-security-resources; Amnesty International, https://www.edx.org/course/digital-security-and-human-rights; Cyberwomen, https://cyber-women.com/en/

[26] IO Foundation, https://www.theiofoundation.org/#Programs; Article 19, https://www.article19.org/resources/ethical-approaches-to-artificial-intelligence-and-autonomous-systems-at-ieee-seas-2017/; IETF Human Rights Protocol Research Group, https://datatracker.ietf.org/rg/hrpc/about/; Cross Community Working Party on ICANN's Corporate and Social Responsibility to Respect Human Rights, https://icannwiki.org/Cross_Community_Working_Party_on_ICANN%27s_Corporate_and_Social_Responsibility_to_Respect_Human_Rights; ISO 26000 Social responsibility, ISO, https://www.iso.org/iso-26000-social-responsibility.html

[27] APNIC, https://academy.apnic.net/en/course/manrs/; CENIC, https://cenic.org/blog/item/cenic-to-explore-adoption-of-manrs

The CBMs recommended in the consensus report adopted by the General Assembly should be implemented by states, including through regional and bilateral mechanisms. There is also a role for civil society organisations to play in their implementation. For example, the CBMs in the report focus on transparency and cooperation measures, such as, facilitating "cross-border cooperation to address critical infrastructure vulnerabilities that transcend national borders" and "development of mechanisms and processes for consultations on the protection of ICT-enabled critical infrastructures". Such processes and mechanisms will require wide stakeholder input - for example, the vast majority of commercial applications today use some open source components, which have been developed by a range of actors, and as such the addressing of threats and vulnerabilities through cross-border coordination will necessitate multistakeholder engagement.

Another CBM included in the 2015 report refers to the setting up of computer emergency response teams, more commonly known as "CSIRTs". A number of multistakeholder initiatives provide best practice guidance in setting up CSIRTs[28].

Further, human rights defenders could through research and monitoring, determine whether CBMs are being implemented in a way that respects human rights. For example, with regards to the CBM which refers to cooperation in investigations related to the use of ICTs for terrorist purposes, civil society has played an essential role in providing guidance and in monitoring such practice to support the carrying out of these investigations in a way which is human rights respecting[29].

---

[28] "Establishing and supporting Computer Incident Security Response Teams (CSIRTs) for Internet security" Internet Governance Forum (IGF) Best Practice Forum on Cybersecurity https://intgovforum.org/multilingual/content/establishing-and-supporting-computer-incident-security-response-teams-csirts-for-internet; "Global Good Practices - National Computer Security Incident Response Teams (CSIRTs)" GFCE, https://www.thegfce.com/documents/publications/2017/11/21/national-computer-security-incident-response-teams-csirts;

[29] "Minimum safeguards on intelligence sharing required under international human rights law", Privacy International, https://privacyinternational.org/advocacy/3068/minimum-safeguards-intelligence-sharing-required-under-international-human-rights-law