DFAT Public Consultation:

Responsible state behaviour in cyberspace in the context of international security at the United Nations

GLOBAL PARTNERS DIGITAL

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.

Contact

Sheetal Kumar
Senior Programme Lead, Global Partners Digital
sheetal@gp-digital.org
+44 (0)20 3 818 3258

---

1. What existing and emerging threats should inform Australia's approach to discussions on the Framework for Responsible State Behaviour in Cyberspace (international law, norms, confidence building measures and capacity building) in the OEWG and GGE?

Most threats in cyberspace are to civilians in peacetime. The OEWG and GGE should support a human-centric and rights-based approach to both identifying and perceiving threats. Ensuring a peaceful and secure cyberspace supports measures which reduce the threat landscape by supporting the security and stability of the internet and digital technologies.

The discussions within the OEWG so far have revealed that threats in cyberspace affect and are perceived by states differently, and that there are increasing links between issues discussed in different forums. Non-government stakeholders have an important role to play in supporting States' well-rounded understanding of the nature and magnitude of threats they face in cyberspace, as well as the relationships and distinctions between threats in cyberspace. In addition, non-government stakeholders can help to address the consequences and the impact of cyber operations on societies and individuals in a way which promotes and protects human rights, and preserves a peaceful, secure and open cyberspace. For example, civil society organisations conduct research and monitoring and can provide data on how cyberthreats and attacks impact their constituencies.

2. Are there any specific areas of the Framework for Responsible State Behaviour in Cyberspace (international law, norms, confidence building measures and capacity building) that, from your perspective, should be further developed in the OEWG/GGE? If so, how would you like to see these areas addressed in any OEWG and/or GGE report(s)?

With regards to the framework for responsible state behaviour, see below our recommendations with regards to capacity building, international law and norms.

3. As stated above, a key Australian objective is for the OEWG and/or GGE to provide practical guidance on observation and implementation of the agreed norms of responsible state behaviour, set out in the 2015 GGE report (found here viii). What do you consider to be best practice observation and implementation of these norms? We welcome your input of concrete examples/suggestions of best practice implementation of one, some, or all of the norms (see Annex A), which could be considered for incorporation into any report of the OEWG and/or GGE.

With regards to best practice in norm implementation, please refer to the following table:

Norm	**Examples of best practice implementation of the Norm**
(a) Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security	There is a mutually reinforcing relationship between the efforts to maintain international peace and security and human rights. Any measures to increase stability and security in the use of ICTs should therefore be human-centric and rights-respecting. Specifically, when it comes to regulatory and policy frameworks in support of stability and security in the use of ICTs – including national cybersecurity strategies and cybersecurity and cybercrime legislation, and relevant international agreements–, these should be rights-respecting and developed in an open, inclusive, and transparent way. Examples of good practices can therefore refer to frameworks that include explicit reference to the link between stability and security in the use of ICTs and human rights.[1] Furthermore, they are likely to include protections for strong technical standards for the

[1] States which have done this in their national cybersecurity strategies include: Canada (2018), Chile (2017), Costa Rica (2017), France (2015), Greece (2018) and Sweden (2017). National strategies can also include objectives or principles, to respect, protect and promote the human rights of persons, include a definition of cybersecurity which is consistent with human rights and international best practice, and if they include a definition of cybercrime, that definition should be consistent with human rights and international best practice.

	protection of data, networks and infrastructure including strong encryption standards and comprehensive data protection legislation.[2] These measures increase stability and security in the use of ICTs in a rights-respecting way. On the other hand, ICT practices which are harmful from a rights-based perspective include arbitrary surveillance, censorship and network disruptions.[3]
(b) In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences;	Although there is currently little available 'best practice' with regards to this norm, attribution in cyberspace is a multidimensional activity and therefore requires interdisciplinary research and multistakeholder engagement. Efforts in this regard, which engage all stakeholders including the technical community and civil society, should be supported. The escalation of tensions between states can harm human rights by leading to increased cyber attacks, which can reduce access to essential services and compromise the integrity of sensitive and personal data.[4] However, attribution in cyberspace is also contested, and processes which occur before public attribution by governments lack transparency, partly due to a reluctance to reveal methods.[5] This contributes to uncertainty, supports deniability and can therefore make deterrence difficult. As a result, independent and trust-building attribution efforts are required.
(c) States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs	This norm refers to the law of state responsibility and the principle of due diligence, which—under international law—obliges a state to not knowingly allow its territory to be used for acts contrary to the rights of other states. It can also be read to refer to the principle under international human rights law that states must protect against human rights abuses within their territory and/or jurisdiction by third parties. It is recommended that states hold private actors who enable or facilitate these acts to account.[6] For example, where there has been misuse of personal data in political campaigns, companies should be investigated and

[2] Association of Progressive Communications and Global Partners Digital, "Unpacking the GGE's framework on responsible state behaviour: Cyber norms"
[3] Ibid
[4] Ibid
[5] Egloff, Florian J. (2019) "Contested public attributions of cyber incidents and the role of academia"
[6] Association of Progressive Communications and Global Partners Digital, Unpacking the GGE's framework on responsible state behaviour: Cyber norms

	brought to account.[7] In addition, the targeting of individuals, including human rights defenders and journalists, using surveillance technology has been shown to lead to "arbitrary detention, sometimes to torture and possibly to extrajudicial killings".[8] States should address the human rights abuses within their territory and/or jurisdiction which occurs as a result of the practices of the largely unregulated private surveillance industry. Seven recommendations to states, including the imposition of an immediate moratorium on the export, sale, transfer, use or servicing of privately developed surveillance tools until a human rights-compliant safeguards regime is in place, are included in the Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (A/HRC/41/35).[9]
(d) States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect;	Best practice with regards to the addressing of cybercrime requires that the state has developed comprehensive legislation – either as a standalone piece of legislation or otherwise – which regulates criminal offences and criminal procedure consistent with the Budapest Convention and international human rights law. An example of cooperation efforts to address related threats and support global coordination on criminal use of ICTs includes constructive engagement in existing discussions, such as the "open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime".[10]
(e) States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to	With regards to this norm, the resolutions referred to provide guidance on actions which states should take in order to comply with the resolutions. These include the adoption of comprehensive human rights legislation (or the existence of provisions in a constitution) which enable individuals to challenge acts which violate their human rights and obtain remedies.

[7] Information Commissioner's Office (ICO) "Investigation into data analytics for political purposes"
[8] Kaye, David, Surveillance and human rights "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression", A/HRC/41/35
[9] Ibid
[10] Open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime

privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression;	States can also recognise in their national cybersecurity strategy, or other documents relating to the secure use of ICTs, the importance of ensuring full respect for human rights.[11] In order to comply with this norm, states could adopt national internet-related public policies that have the objective of universal access and enjoyment of human rights at their core (HRC Res. 26/13) and take steps to identify and bridge any digital divides that exist in the state (HRC 32/13). This includes adopting measures, including legislative measures, to ensure that persons with disabilities are able to access information and communications technology and systems on an equal basis with others (HRC 32/13) and promote digital literacy among its population (HRC 26/13). The state should also prohibit measures which intentionally prevent or disrupt access to or dissemination of information online or publicly commit not to take such measures (HRC 32/13). It should also adopt a comprehensive legislative framework on surveillance and other investigatory powers, consistent with international standards and best practice, and which include independent oversight, grievance mechanisms and access to remedy (UNGA 68/167). States should adopt a comprehensive legislative framework on data protection with international standards and best practice such as Council of Europe's Convention No. 108 and the OECD Privacy Guidelines, and which include independent oversight, grievance mechanisms and access to remedy (UNGA 68/167).
(f) A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public;	See recommendations with regards to critical infrastructure protection below.

[11] In particular, states can explicitly recognise the role that cybersecurity plays in protecting human rights in national cybersecurity strategies. See footnote 1 for examples.

(g) States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions;	A range of good practices resources exist to provide guidance on appropriate measures to protect critical infrastructure (CIP). These include those developed by multistakeholder initiatives, including the Global Forum on Cyber Expertise (GFCE), in collaboration with the Meridian process.[12] They include reference to the importance of clearly defining critical infrastructure and engaging a wide range of stakeholders, including the technical community and civil society, due to the complex nature of the threat landscape. These resources recognise that the identification and protection of critical information infrastructure (CII) should also be considered alongside CIP as critical infrastructure is increasingly dependent on ICTs. The importance of clearly identifying the critical elements of both a state's CII and critical information infrastructures (CII) elements of critical infrastructure is emphasised in the good practice guidance available from the GFCE. This includes the importance of a coordinated approach between all actors involved in CIIP and CIP. An example of a multi-layered, intra-sector and coordinated approach, which integrates the protection of CII and CI is provided by Estonia's CIP policy.[13] Personal data, including sensitive personal data, is often compromised as a result of incidents which affect CII and or/CI. At the same time access and monitoring of data is required to identify and manage risks. Therefore, it's important to recognise that CIIP and/or CIP policies should be consistent with privacy and data protection regulations.[14]For example, sharing of information on risks and incidents to the national competent authorities might require processing of personal data and therefore should comply with privacy and data protection regulations and protect the right to privacy.
(h) States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at	As mentioned above, personal data, including sensitive personal data, is often compromised as a result of incidents which affect CII and or/CI. Information sharing mechanisms across borders should be in compliance with international human rights law, and reflect trust conditions referred to in the "OECD Council's Recommendation on Digital Security of Critical Activities"[15] and the EU's "Directive on security of network and information

[12] GFCE, "Global Good Practices - Critical Information Infrastructure Protection"; the GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers; Companion Document to the GFCE-MERIDIAN Guide on CIIP
[13] GFCE, Companion Document to the GFCE-MERIDIAN Guide on CIIP
[14] OECD (2019) "Recommendation on Digital Security of Critical Activities",

[15] Ibid

the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty;	systems".[16]
(i) States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions;	Ensuring the integrity of the supply chain requires that states refrain from mandating backdoor access to ICT products (hardware and software) and in popular communication platforms. Additionally, this norm is about preventing the proliferation of malicious ICTs and techniques.[17] Malware and software vulnerabilities which are used to target HRDs have been disseminated through app stores and software updates. As mentioned above in relation to norm (a), it is crucial for the peace and stability of cyberspace that states promote measures which increase the stability and security of ICTs. This requires measures which protect, instead of weaken, strong encryption as weak encryption can introduce vulnerabilities into the supply chain, and contribute to the proliferation of malicious ICT tools and techniques. States should support privacy by design in the supply chain including via multistakeholder initiatives such as the Online Trust Alliance to develop and advance best practices to protect users' security, privacy, and identity.[18] Other steps states can take to support supply chain integrity include the conduct of human rights impact assessments[19] and the inclusion of supply chain security and steps taken to mitigate against the proliferation of malicious ICT tools and techniques in National Action Plans (NAPs).[20]
(j) States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure;	Responsible reporting of ICT vulnerabilities, which in some cases have been the main mechanism for conducting cyber operations, is essential for maintaining a peaceful and secure cyberspace. As the use of shared ICT systems, including as a result of the spread of connected devices, continues, the existence of ICT vulnerabilities and the need to address them in a timely manner grows in urgency. Due to the varied equities and responsibilities of

[16] European Commission, "The Directive on security of network and information systems (NIS Directive)"
[17] Association of Progressive Communications and Global Partners Digital, "Unpacking the GGE's framework on responsible state behaviour: Cyber norms"
[18] Internet Society, Online Trust Alliance
[19] Article 19, "Assessing the Human Rights Impact of Internet Registries"
[20] Some examples of states that have included reference to the mitigation options for avoiding or reducing human rights risks associated with ICTs in their NAPs include Luxembourg and the UK, National Action Plans on Business and Human Rights

	stakeholders with regards to vulnerability reporting,[21] states should recognise and institute disclosure processes that recognise that vulnerability reporting is a multistakeholder effort and thus engage all stakeholders in both the development and implementation of vulnerability disclosure processes. States should make public the criteria and processes used in determining whether the government discloses a vulnerability they have discovered[22] and should codify government disclosure processes into law to ensure compliance.[23] In addition, states should set up coordinated vulnerability disclosure processes,[24] to engage all stakeholders in vulnerability reporting, in accordance with the guidelines and recommendations defined in ISO/IEC 29147:2014 and ISO/IEC 3011.[25] In particular, best practice guidance highlights the importance of both protecting and incentivising the work of security researchers. To this end, national legislation should be amended to protect security researchers and provide them with legal certainty in reporting vulnerabilities.[26] Complementary best practice programmes which states can promote to raise awareness of the importance of disclosure and to incentivise disclosure of vulnerabilities include the promotion of "safe harbor policies",[27] and "bug bounty programmes".[28] States should also fund defensive

[21] CEPs (2018) "Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges"; ENISA (2016) "Good Practice Guide on Vulnerability Disclosure: From Challenges to recommendations"; Global Forum on Cyber Expertise (2017) "Global Good Practices - Coordinated Vulnerability Disclosure (CVD)"

[22] Examples include: Australia, Responsible Release Principles for Cyber Security Vulnerabilities, United Kingdom Government Communications Headquarters, the Equities Process; United States, Vulnerabilities Equities Policy and Process for the United States Government

[23] CEPs (2018) "Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges"

[24] United Kingdom, National Cyber Security Centre, Vulnerability Reporting, "How to report a vulnerability in a UK government website or system"

[25] ISO/IEC 29147:2014 [ISO/IEC 29147:2014], Information technology — Security techniques — Vulnerability disclosure; ISO/IEC 30111:2013 [ISO/IEC 30111:2013] Information technology — Security techniques — Vulnerability handling processes

[26] The Netherlands provides an example of a regulatory framework for vulnerability reporting which provides legal certainty to researchers, CEPs (2018) "Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges"

[27] Mozilla, "Safe Harbor for Security Bug Bounty Participants"; Microsoft, "Microsoft Bounty Legal Safe Harbor"

[28] Singapore GovTech (2019) "Third Government Bug Bounty Programme offers bonus payouts for mobile applications"; Government of the Netherlands, "Responsible disclosure"

	vulnerability discovery and research and invest in building security researcher communities.
(k) States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.	Incident response requires quick information sharing, which is dependent on strong relationships between the actors involved. A degree of independence and transparency between computer incident response teams (CERTs) and parts of government is important from a rights perspective, to ensure that a CERT carries out its work without impinging on freedom of expression or privacy.[29] Best practice observation of this norm should consider both authorised and non-authorised emergency response teams as CERTs vary widely globally in their independence and relationship to government actors. States should consider the recommendations from CERT networks on how to best support CERT activities, including the contribution of FIRST, the global network of CERTs, to the OEWG.[30]

Discussions within the OEWG so far have highlighted commitment to operationalising the existing eleven GGE norms but equally highlighted gaps in awareness of the norms and capacity to implement them. We would also emphasise that efforts to operationalise norms exist around the world. Multistakeholder efforts by the Internet Governance Forum's Best Practice Forum (BPF) and the Global Forum on Cyber Expertise (GFCE) should be consulted and these should be examined, captured, and built upon.

In addition, a mechanism to support the periodic review of implementation of the eleven norms would allow for the capturing of lessons learned, as well as increase awareness of the norms, build trust and confidence, create incentives for compliance and thereby ensure the observation of norms. Assessments of norm implementation should be periodic and publicly available as well as permit non-government stakeholders to participate.

While the emphasis in the OEWG and GGE should be on implementing the existing norms and ensuring transparency and inclusiveness in their implementation, any development of further norms should be inclusive of all stakeholders, and should refer to existing efforts, in particular the norms developed by the Global Commission on the Stability of Cyberspace (GCSC) in order to promote consistency and build on existing efforts.

[29] Association of Progressive Communications and Global Partners Digital, Unpacking the GGE's framework on responsible state behaviour: Cyber norms

[30] FIRST, 2019, "Position paper by the Forum of Incident Response and Security Teams on cybersecurity developments within the UN context"

4. The mandate of the GGE invites members to annex to the GGE report "national contributions…on the subject of how international law applies to the use of information and communications technologies by States". Through the International Cyber Engagement Strategy, Australia has published its positions on the application of international law to cyberspace in 2017 and 2019 (found here ix). Are there any relevant areas of international law that that, from your perspective, should be addressed in any Australian contribution to the international law annex to the GGE report? If so, how would you like to see these areas addressed?

Australia has recognised that international law in cyberspace includes international humanitarian law and international human rights law. In order to promote greater clarity on how international human rights law applies in cyberspace, Australia could provide examples of how international law can be interpreted in reference to international human rights law. It should also encourage other states to underpin their interpretations of international law in a way that reinforce human rights obligations and human-centric interpretations of international law.

5. Another key Australian objective is for any report of the OEWG and/or GGE to make recommendations on better coordinating global cyber capacity building. We welcome suggestions on how coordination of global cyber capacity building might be improved, as well as how you would like this to be addressed in any OEWG and/or GGE report(s).

Capacity building is key to reducing threats, operationalising norms and improving trust, confidence and ultimately peace and security in cyberspace. However, in order for capacity building to achieve these aims, we recommend that Australia:

- Invest in resources in improving existing coordination and information sharing mechanisms and spaces at the global level, including the GFCE
- Adopt a holistic approach to cybersecurity capacity building that aims to build capacity in a sustainable way.[31] This includes ensuring local ownership by using a bottom-up approach to capacity building in order to foster local ownership and buy-in[32]

---

[31] For example, GPD delivers cyber capacity building projects which embed a strategic approach to engaging in cyber policy debates within the institutional fabric of partner organisations, rather than just working with individuals within the partner organisations. In this way, partners are encouraged to build cyber policy issues into their existing agendas and long-term organisational strategies. To complement these capacity building efforts, GPD fosters networks in target regions (as well as globally), thus creating a support system that can transcend the project cycle. Project outputs have raised awareness of the implications of cyber policy issues on human rights and democracy among key decision-makers. The knowledge and skills built, as well as the training tools developed as part of its implementation, have enabled groups to engage more effectively in cybersecurity discussions beyond the project cycle.

[32] Response exercises include the annual APCERT Cyber Drill; other initiatives include the establishment or strengthening of national incident response networks such as PaCSON; and national initiatives to establish CSIRTs

- Facilitate a diversity of representation, particularly from the global South, in global forums
- Identify and foster champions through 'train the trainers' initiatives[33]
- Foster initiatives that seek to operationalise commitments to multi-stakeholder approaches to cyber policy development and capture good practices.

6. What role should the business/government/NGO/academic community play in promoting a peaceful and stable online environment? How would you like to see this addressed in any OEWG and/or GGE report(s),or any Australian contribution to the annex to the GGE report?

The OEWG, GGE and Australian contribution should acknowledge that addressing the nature of threats to a peaceful and secure cyberspace will require an open, inclusive, multistakeholder approach. Non-governmental stakeholders, including civil society, play vital and varied roles in promoting a peaceful and stable online environment and this should be acknowledged in the report. This includes but is not limited to research and monitoring, capacity-building, providing evidence-based research, developing and implementing technical and policy standards which includes providing recommendations on how to implement international commitments and regulatory frameworks for the national context in a rights-respecting and context-specific manner.

Civil society has important and wide-ranging roles to play in implementing the concrete measures included in the 2015 GGE framework for responsible state behaviour, including in implementing the eleven norms, carrying out capacity building activities, and ensuring that the implementation of confidence-building measures are human-rights compliant. The OEWG and GGE reports, and any Australian contribution to the annex to the GGE report could include concrete examples of non-government stakeholder implementation of the 2015 GGE framework, some of which are included in GPD's contribution to the OEWG intersessional meeting.[34]

Further efforts are required to outline the roles and responsibilities of stakeholders in the implementation of the eleven GGE norms. In order to do so, Australia could refer to existing efforts including the Geneva Dialogue on Responsible Behaviour in Cyberspace,[35] the Australian Strategic Policy Institute's ASEAN workshop on implementation of norms (November 2019), and a recent EU Cyber Direct workshop.[36]

---

[33] Examples include APNIC's training program for local network operators in Asia/Pacific, and good practice development, training, and fellowships by the Forum for Incident Response and Security Teams (FIRST)

[34] Global Partners Digital, 2019, "Submission by Global Partners Digital to the Informal intersessional consultative meeting of the OEWG with industry, non-governmental organizations and academia (2-4 December 2019)"

[35] Geneva Dialogue on Responsible State Behaviour

[36] EU Cyber Direct (2019) "Strengthening the Multistakeholder Approach on Norms in Cyberspace"