



PUBLIC CONSULTATION: RESPONSIBLE STATE BEHAVIOUR IN CYBERSPACE IN THE CONTEXT OF INTERNATIONAL SECURITY AT THE UNITED NATIONS

OVERVIEW

The Department of Foreign Affairs and Trade (DFAT) is calling for submissions to inform Australia's engagement in two United Nations (UN) processes on responsible state behaviour in cyberspace.

In December 2018, the United National General Assembly (UNGA) established two processes: an inaugural *Open Ended Working Group on developments in the field of information and telecommunications in the context of international security* (OEWG) ([A/Res/73/27](#));ⁱ and, a sixth *Group of Governmental Experts on advancing responsible state behaviour in cyberspace in the context of international security* (GGE) ([A/Res/73/266](#)).ⁱⁱ

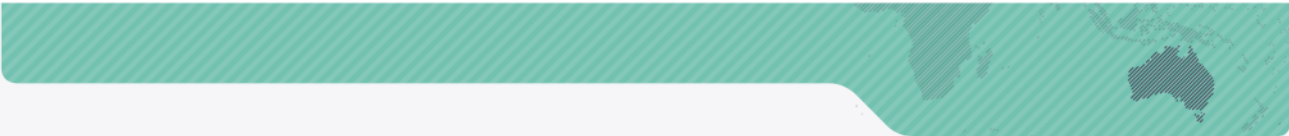
The groups present an important opportunity to promote a peaceful and stable online environment and enhance international security. Australia is a member of both groups.

BACKGROUND: FRAMEWORK FOR RESPONSIBLE STATE BEHAVIOUR IN CYBERSPACE

Cumulatively the 2010, 2013 and 2015 GGE outcome reports ([A/65/201](#),ⁱⁱⁱ [A/68/98](#),^{iv} and [A/70/174](#)^v) affirm that existing international law – and in particular, the Charter of the United Nations in its entirety – is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment. The reports also articulate voluntary non-binding norms of responsible state behaviour, while recognising the need for confidence building measures (CBMs), and coordinated capacity building. Combined, these measures (international law, norms, CBMs and capacity building) provide the basis for a peaceful and stable cyberspace, and are often referred to as a Framework for Responsible State Behaviour in Cyberspace (the Framework).

Australia reaffirms its commitment to act in accordance with the cumulative GGE reports from 2010, 2013 and 2015. Recalling that in 2015 the UNGA called on all UN Member States 'to be guided in their use of information and communications technologies by the [GGE's] 2015 report' ([A/RES/70/237](#)^{vi}), the links on [this webpage](#)^{vii} provide an overview of how Australia observes and implements the four pillars of the Framework.

A key Australian objective is for the inaugural OEWG and/or the sixth GGE to provide practical guidance on implementation of the agreed norms of responsible state behaviour, backed up by recommendations on better coordinating global cyber capacity building, so that all countries are in a position to observe and implement the Framework.



CALL FOR SUBMISSIONS:

DFAT encourages interested individuals and organisations to make written submissions in relation to Australia's priorities for the OEWG and GGE.

Written submissions should be lodged by close of business **28 January 2020**. Submissions should include your full name, email address and telephone number. Electronic lodgement is preferred.

Submissions may range from a short email or letter, outlining your views on a particular topic, to a more substantial document covering a range of issues. Where possible, you should provide evidence, such as relevant data and documentation, to support your views

Submissions should be sent via email to: CyberAffairs@dfat.gov.au.

In your submission, you might consider answering one or more of the following questions:

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?
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)?
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.
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?
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).
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?



YOUR SUBMISSION AND CONFIDENTIALITY:

All submissions will be published as public documents on the DFAT website. However, information which is of a confidential nature or which is submitted in-confidence, will be treated as such by DFAT, provided the basis for such treatment is provided.

DFAT may also request that a non-confidential summary of the confidential material is provided, or reasons why a summary cannot be provided.

Material supplied in-confidence should be clearly marked 'IN CONFIDENCE' and be in a separate attachment to non-confidential material.

ⁱ <https://dfat.gov.au/international-relations/themes/cyber-affairs/Documents/2018-first-committee-russian-resolution.pdf>

ⁱⁱ <https://dfat.gov.au/international-relations/themes/cyber-affairs/Documents/2018-first-committee-us-resolution.pdf>

ⁱⁱⁱ <https://dfat.gov.au/international-relations/themes/cyber-affairs/Documents/ungge-2010-a65201.pdf>

^{iv} <https://dfat.gov.au/international-relations/themes/cyber-affairs/Documents/ungge-2013-a6898.pdf>

^v <https://dfat.gov.au/international-relations/themes/cyber-affairs/Documents/ungge-2015-a70174.pdf>

^{vi} <https://dfat.gov.au/international-relations/themes/cyber-affairs/Documents/ungge-2015-a-res-70-237.pdf>

^{vii} <https://dfat.gov.au/international-relations/themes/cyber-affairs/Pages/international-security-and-cyberspace.aspx>

^{viii} <https://dfat.gov.au/international-relations/themes/cyber-affairs/Documents/ungge-2015-a70174.pdf>

^{ix} <https://dfat.gov.au/international-relations/themes/cyber-affairs/Documents/application-of-international-law-to-cyberspace.pdf>



Australian Government

Department of Foreign Affairs and Trade


Annex A: Public Consultation: Responsible state behaviour in cyberspace in the context of international security at the United Nations

Developing Best Practice Guidance on implementation of the 11 norms of responsible state behaviour in cyberspace articulated in the 2015 GGE Report ([A/70/174](#)), as endorsed by the UN General Assembly ([A/RES/70/237](#))

Respondents may wish to review the table (available [here](#)) which sets out how Australia currently implements each of the norms from the 2015 GGE Report.

Input of concrete examples/suggestions of best practice implementation of one, some, or all of the norms in the table below is welcomed:

Norm	Examples of best practice implementation of the Norm
<i>Taking into account existing and emerging threats, risks and vulnerabilities, and building upon the assessments and recommendations contained in the 2010 and 2013 reports of the previous Groups, the present Group offers the following recommendations for consideration by States for voluntary, non-binding norms, rules or principles of responsible behaviour of States aimed at promoting an open, secure, stable, accessible and peaceful ICT environment:</i>	
<i>(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</i>	
<i>(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;</i>	



<i>(c) States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs</i>	
<i>(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;</i>	
<i>(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 privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression;</i>	
<i>(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;</i>	
<i>(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;</i>	
<i>(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</i>	



<i>activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty;</i>	
<i>(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;</i>	
<i>(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;</i>	