29 May 2020

Submission of Australia's independent expert to the United Nations Group of Governmental Experts on advancing responsible State behaviour in cyberspace in the context of international security (GGE), Ms Johanna Weaver

This submission provides commentary and non-exhaustive examples of best practice implementation of the eleven norms of responsible state behaviour agreed in 2015 GGE Report (A/70/174), as endorsed by all UN member states in UN General Assembly resolution A/RES/70/237.

All text in italics is taken directly from the 2015 GGE Report. All other text represents the views of Ms Weaver.

Examples of how the Australian Government implements each of the 2015 GGE norms can be found in Annex B to Australia's National Paper to the Open Ended Working Group on the use of ICTs in the context of international security (OEWG).[1]

Norm	Commentary on the norm	Examples of best-practice implementation of the norm by States
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,	This chapeau paragraph underscores that the norms are voluntary and non-binding. That said, all States have agreed 'to be guided in their use of information and communications technologies by the [UNGGE's] 2015 report' (A/RES/70/237). Norms complement existing international law. When considering (and respecting) their obligations under existing international law, States should also give consideration to the application of the voluntary non-binding norms.	

[1] Available at https://www.dfat.gov.au/international-relations/themes/cyber-affairs/Pages/international-security-and-cyberspace

Norm	Commentary on the norm	Examples of best-practice implementation of the norm by States
accessible and peaceful ICT environment:		

(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;	States do – and should – cooperate on many issues (writ large). States do – and should – cooperate on many issues that fall within cyber and digital agenda. Cooperation in the context of this norm is specific, the purpose of this cooperation is 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.
	
	Cooperation should be with the full spectrum of actors across government (foreign policy, trade, technical, national security, law enforcement, military, and political), as well as with the private sector and multi-stakeholder community.
	
	Transparency (publishing documents and doctrine and sharing approaches to addressing threats or harmful ICT practices), even where no direct cooperation takes place, can also help build trust and confidence between States.
		Establish a unit within the Ministry of Foreign Affairs with responsibility to coordinate whole-of-government international cooperation on issues pertaining to international peace and security in cyberspace.
		
		Initiate bilateral/trilateral/plurilateral cyber policy dialogues that foster discussion on issues of international peace and security in cyberspace.
		
		Participate in relevant regional and global multilateral meetings (such as ASEAN Regional Forum Intersessional Meeting on ICT Security, and the UN GGE and OEWG).
		
		Publish and share government policy on issues pertaining to international peace and security in cyberspace. Such documents should link international efforts to domestic efforts, and provide for meaningful multi-stakeholder engagement.

(b) In case of ICT incidents, States should consider all relevant information, including the larger context of the event,	This norm encourages States to take into account a number of factors when considering how best to respond to ICT incidents with the potential to threaten international peace and stability.	Develop a national cyber incident classification methodology, to foster consistent incident severity categorisation.

Norm	Commentary on the norm	Examples of best-practice implementation of the norm by States
the challenges of attribution in the ICT environment and the nature and extent of the consequences;	ICT incidents should not be seen in technical isolation but placed within the larger context, including the broad factual circumstances and strategic bilateral, regional and global dynamics. Attribution* of ICT incidents is complex, but it is not impossible. Whole-of-government coordination will be required as different organisations hold different pieces of the attribution puzzle. States should also consider if the private sector holds relevant information. Not all countries have technical attribution capabilities, capacity building should be considered upon request (noting there may also be a role for private sector). * States should make the distinction between different attribution assessments, including factual attribution assessments (which includes an assessment of technical and other contextual information) and legal attribution assessments (whether there has been a breach of international law and/or domestic law),** as well as the political decision to act – publicly or privately – on those attribution assessments. **With respect to legal attribution assessments, the customary international law on State responsibility provides that a State will be responsible for an internationally wrongful act where there is conduct (whether by act or omission) that is attributable to it and that conduct constitutes a breach of its international obligations. Not all ICT incidents will threaten international peace and security; responses need to be calibrated according to the	Develop and exercise national cyber incident management arrangements, to define roles and responsibilities across government including with respect to the most severe cyber-incidents (i.e.: those that may pose a threat to international peace and security). Establish and maintain information sharing arrangements with global CERT and cyber security counterparts, to facilitate technical information sharing and cooperation during cyber incidents. These arrangement should seek to leverage the resources, experience and expertise from all relevant stakeholders – including from industry and civil society/academia. Develop a whole-of-government attribution framework to guide and inform decisions by government to publicly or privately make attribution disclosures (taking into account the different types of attribution assessments, see: commentary (left), and noting that public attribution may be deployed in conjunction with, or in lieu of, other responses). Review options available to government to respond to significant cyber incidents and develop a policy for their deployment. Options could encompass diplomatic, economic, legal & law enforcement, defence-based, and private sector measures. Publish national views on the application of international law to cyber incidents, responses and remedies.

Norm	Commentary on the norm	Examples of best-practice implementation of the norm by States
	nature and severity of the incident. Any action taken by a State in response to an ICT incident should be appropriate and proportionate to the relevant ICT incident. Transparency about the policies and procedures that inform operational and strategic responses to cyber incidents will promote common understandings, increase predictability, foster trust and reduces the risk of miscommunication during times of crisis.	
(c) States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;	This norm is sometimes referred to as the "due diligence norm". While there is no international consensus on whether due diligence is an international legal obligation applicable to State conduct in cyberspace, this norm has had universal endorsement (via A/Res/70/237). "Internationally wrongful act" (IWA) is a specific legal term, with two elements: 1. an act or omission attributable to the State under international law 2. that breaches an international legal obligation of the State (including a breach of a treaty obligation or a breach of customary international law). These elements are settled customary international law and are reflected in Article 2 of the International Law Commission's Articles on the Responsibility of States for Internationally Wrongful Acts. The norm requires that both of these criteria must first be met.	Publicly reaffirm (for example in ministerial statements and policy documents) the commitment to act in accordance with all of the recommendations of the 2015 GGE Report, including this norm, and refrain from conduct in contravention of this norm. Establish comprehensive domestic offences to combat cybercrime, for example: those provided for in the Council of Europe Convention on Cybercrime (the Budapest Convention). Offenses should be drafted in a technology neutral manner, so as to accommodate future advances in technology. Maintain national and international coordination mechanisms to facilitate detection and prosecution of cybercrime offenses (see also Norm D below). Publish national views on what constitutes an internationally wrongful act using ICTs, and on what a State should do if it is aware of an internationally wrongful act originating from, or routed through, its territory.

Norm	Commentary on the norm	Examples of best-practice implementation of the norm by States
	An act will be attributable to a State under customary international law where, for example, it was conducted by an organ of the State; by persons or entities exercising elements of governmental authority; or by non-State actors operating under the direction or control of the State. The norm provides that States should take certain action where it knows or is aware of the IWA occurring within its territorial borders. In this context, knowledge is linked to capacity. What a developed State "knows" may be different to what a developing State "knows"; therefore, what satisfies the standard for each may be different. The capability of a State could also affect what sort of action it should take in response to an internationally wrongful act on its territory. It may not be reasonable to expect (or even possible for) a State to prevent all malicious use of ICT infrastructure located within its territory. The norm requires that States take reasonable steps, consistent with their capabilities, to end the harmful activity. This norm does not require that a State proactively monitor all ICTs within its territory or take other preventative steps. Knowledge is also linked to notice. If a State is notified of the activity it should act, within its capacity and consistent with international law. Of course, a State may have "knowledge" of relevant conduct without having been notified of it.	Develop transparent procedures to respond to appropriate notifications from other governments (see also Norm H below).
(d) States should consider how best to cooperate to exchange information, assist each other,	An absence of cooperation among States when prosecuting terrorist and criminal use of ICTs could be destabilizing and lead to mistrust among states. Other UN fora lead on	See Norm C (above) for best practice on domestic legislative frameworks.

Norm	Commentary on the norm	Examples of best-practice implementation of the norm by States
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;	cooperative responses to cybercrime and terrorist use of ICTs; this norm therefore necessarily focuses on the importance to international stability of this cooperation. This norm is not just about terrorist and criminal use of ICTs: at its heart it is a norm about information exchange. Computer Emergency Response Teams (CERTs) play a vital role in exchange of technical information (it is important this work remains apolitical). States should also have domestic and international policies and procedures in place to respond to requests for assistance in a manner compliant with its international human rights obligations, including technical/law enforcement/legal/ national security/military cooperation. All cooperation to prosecute terrorist and criminal use of ICTs should be consistent with States' international human rights obligations. The norm also reflects that States may need to consider whether new measures need to be developed in this respect.	Establish units within national agencies with responsibility for investigating and prosecuting criminal and terrorist use of ICTs, consistent with States' international human rights obligations, and in coordination with whole of government and industry partners. Maintain mechanisms to coordinate and share information with international partners, consistent with States' international human rights obligations (for example: through membership of Interpol and ratification of Budapest Convention, which provides means for mutual legal assistance and a 24/7 Network for Parties to assist investigations and secure electronic evidence efficiently). Build relationships with the private sector as well as civil society and academia (especially those with access to relevant data, information & expertise to combat criminal activity online), ensuring appropriate human rights protections. Participate in multilateral cybercrime processes, including, for example: UN Commission on Crime Prevention and Criminal Justice (CCPCJ), UN Open-Ended Intergovernmental Expert Group on Cybercrime (IEG). Support capacity building to strengthen legislative frameworks and institutional capacity to prevent, investigate and prosecute cybercrime and terrorist use of ICTs consistent with States' international human rights obligations. Participate in multilateral processes providing guidance on preventing terrorist use of the internet, including, for

Norm	Commentary on the norm	Examples of best-practice implementation of the norm by States
		example: Global Internet Forum on Counter-Terrorism (GIFCT), the Global Counter Terrorism Forum; the Aqaba Process, the OECD, and G20 (including the Osaka Leaders' Statement on Preventing Exploitation of the Internet for Terrorism and Violent Extremism Conducive to Terrorism). Subscribe to the Christchurch Call to Action.
(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;	The UN General Assembly has recognised, by consensus, that human rights should be protected online, just as they are offline (A/RES/68/167). The resolutions referenced in this norm have been endorsed by members of the Human Rights Council and General Assembly respectively. The resolutions provide guidance on actions States should take in order to implement the resolutions. States should not compromise the protection of human rights in the name of ICT security. Recalling and endorsing comments to this effect in the 2016 Freedom Online Coalition 'Statement on a Human Rights Based Approach to Cybersecurity Policy Making': "Regrettably, the prevalent worldview is to see human rights and cybersecurity interests in absolute terms – one must be traded-off in the favour of the other…human rights and cybersecurity are complementary, mutually reinforcing and interdependent. Both are essential for the promotion of freedom and security…[T]here is a pressing need to move beyond the dominant rights versus cybersecurity paradigm, by recognising that individual security is a core component of	Publicly reaffirm (for example in ministerial statements and policy documents) that human rights apply online, just as they do offline. Adopt and/or confirm the application of existing domestic legislative, regulatory frameworks and oversight bodies to ensure the promotion, protection and enjoyment of human rights online consistent with international obligations. Publish national views on how international human rights law applies in cyberspace. Participate in multilateral processes with a view to developing common understandings of the application of international obligations to State conduct in cyberspace, including, for example: the UN Human Rights Council. To better understand how particular polices might impact the ability of individuals to exercise their human rights, consult with industry, civil society, and academia when adopting cybersecurity policies and approaches domestically; and engage with groups such as Freedom Online Coalition internationally.

Norm	Commentary on the norm	Examples of best-practice implementation of the norm by States
	cybersecurity and that a secure Internet is central to promoting human rights."	
(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;	This norm encompasses activities conducted by the State itself. Further, the reference to "knowingly support" provides that States cannot evade the application of this norm by using proxies (see also paragraph 28(e) of the 2015 GGE Report) In order to be "contrary to its obligations under international law" the activity must be an act attributable to a State under international law (see note ** to Norm B above) that violates one of its international obligations (including a breach of a treaty obligation or a breach of customary international law). Different States have different national priorities and methods of categorisation of critical infrastructure. In addition some States are reticent to emphasise particular categories of critical infrastructure, lest it be seen to implicitly condone malicious activity against a category not specified. If the GGE chooses to highlight specific types of critical infrastructure (for example, health and emergency coordination infrastructure) it should be underscored that the highlighted sectors are non-exhaustive and do not impact on the national designation, or not, of any sector, nor does it implicitly condone malicious activity against a category not specified.	Publicly reaffirm (for example in ministerial statements and policy documents) the commitment to act in accordance with all of the recommendations of the 2015 GGE report, including this norm, and refrain from conduct in contravention of this norm. If a State has such capabilities, make public statements about the conduct and authorisation of offensive cyber capabilities, reaffirming a commitment to always act consistent with obligations at domestic and international law, and subject to a comprehensive review and oversight framework. Acknowledgment of these capabilities does not contradict a commitment to a peaceful and stable online environment. Instead, by being transparent about the legal frameworks that govern their use, States send an unambiguous message that States' activities in cyberspace have limitations and are subject to obligations, just as they are in the physical domain. States should be unequivocal in their commitment to develop and use ICTs in accordance with international law, as well as norms of responsible State behaviour agreed at the UN.
(g) States should take appropriate measures to protect their critical	Different States have different national priorities and methods of categorisation of critical infrastructure (see Norm F above). What is critical infrastructure for one State, may	Annex A of General Assembly resolution 58/199 (which is a consensus resolution) set out "Elements for protecting

Norm	Commentary on the norm	Examples of best-practice implementation of the norm by States
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;	not be critical infrastructure for another. Designation of critical infrastructure will evolve over time. This norm provides that each State should determine what infrastructure it considers to be critical and take appropriate measures to protect it. Annex A of the resolution referred in the norm provides guidance on "appropriate measures".	critical information infrastructure" (including a road map for domestic implementation); recommendations include: "1. Have emergency warning networks regarding cyber-vulnerabilities, threats and incidents. 2. Raise awareness to facilitate stakeholders' understanding of the nature and extent of their critical information infrastructures and the role each must play in protecting them. 3. Examine infrastructures and identify interdependencies among them, thereby enhancing the protection of such infrastructures. 4. Promote partnerships among stakeholders, both public and private, to share and analyse critical infrastructure information in order to prevent, investigate and respond to damage to or attacks on such infrastructures. 5. Create and maintain crisis communication networks and test them to ensure that they will remain secure and stable in emergency situations. 6. Ensure that data availability policies take into account the need to protect critical information infrastructures. 7. Facilitate the tracing of attacks on critical information infrastructures and, where appropriate, the disclosure of tracing information to other States. 8. Conduct 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. 9. Have adequate substantive and procedural laws and trained personnel to enable States to investigate and prosecute attacks on critical information infrastructures and to coordinate such investigations with other States, as appropriate.

Norm	Commentary on the norm	Examples of best-practice implementation of the norm by States
		10. Engage in international cooperation, when appropriate, to secure critical information infrastructures, including by developing and coordinating emergency warning systems, sharing and analysing information regarding vulnerabilities, threats and incidents and coordinating investigations of attacks on such infrastructures in accordance with domestic laws. 11. Promote national and international research and development and encourage the application of security technologies that meet international standards."
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 the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty;	ICT activity in the context of this (and all the norms) is ICT activity with the potential to threaten international peace and stability. States should respond to appropriate requests for assistance from a State the critical infrastructure of which is being targeted and offer any assistance in accordance with international law that they have the capacity and available resources to provide. As with Norm C (above), it may not be reasonable to expect (or even possible for) a State to prevent all malicious use of ICT infrastructure located within its territory. The norm requires that States respond to appropriate requests by taking reasonable steps, consistent with their capabilities, to end the harmful activity. In doing so states may minimise misperceptions and help restore trust. A State is not required to proactively monitor all ICTs within its territory or take other preventative steps.	To implement this norm States should, upon receipt of an appropriate request for assistance: • acknowledge receipt of the request; • determine, in a timely fashion, whether it has the capacity and resources to provide the assistance requested; • if it is able to assist, indicate the nature, scope and terms of the assistance that might be provided.

Norm	Commentary on the norm	Examples of best-practice implementation of the norm by States
(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;	A key source of vulnerability of ICT products is in the supply of equipment, services and support arrangements, often referred to as supply chain risk. Effective cyber supply chain risk management ensures, as much as possible, the secure supply of products and services for systems throughout their lifetime. For products, this includes their design, manufacture, delivery, maintenance and disposal. As with all norms, this norm considers supply chain risk in the context of international peace and stability. The following extracts from the Prague Proposals may be of relevance: "Shared responsibility of all stakeholders should drive supply chain security…Major security risks emanate from the cross-border complexities of an increasingly global supply chain which provides ICT equipment. These risks should be considered as part of the risk assessment based on relevant information and should seek to prevent proliferation of compromised devices and the use of malicious code and functions… [ICT products] should be designed with resilience and security in mind. They should be built and maintained using international, open, consensus based standards and risk-informed cybersecurity best practices. Clear globally interoperable cyber security guidance that would support cyber security products and services in increasing resilience of all stakeholders should be promoted.	Publish advice on supply chain risk management. Participate in international arrangements for mutual recognition of certified products and service, like the Common Criteria initiative. Participate in the Wassenaar Arrangement on the transparency of dual-use goods and technologies. Prohibit building or implementing systemic weaknesses or vulnerabilities (often called 'backdoors') in ICT products. Take into account the multi-use nature of ICT products and role of cybersecurity researchers and penetration testers when implementing measures to prevent the proliferation of malicious ICT tools and harmful hidden functions.

Norm	Commentary on the norm	Examples of best-practice implementation of the norm by States
	Every country is free, in accordance with international law, to set its own national security and law enforcement requirements, which should respect privacy and adhere to laws protecting information from improper collection and misuse. Laws and policies governing networks and connectivity services should be guided by the principles of transparency and equitability, taking into account the global economy and interoperable rules, with sufficient oversight and respect for the rule of law."	
(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 vulnerabilities limits potential threats to ICTs and ICT-dependant infrastructure. States should have a framework in place to guide national decisions on the handling of ICT vulnerabilities. This is not just the responsibility of governments, but also industry (to better integrate security by design, develop private sector vulnerability disclosure processes, and commit to rapid mitigation of identified vulnerabilities), and technical experts, cyber security companies, researchers and penetration testers (to responsibly report and share vulnerability information). Coordination within and across these communities is important.	Develop - and publicly release - a national vulnerability disclosure framework/vulnerability equities process, to guide national vulnerability disclosure decisions. Support coordinated multi-stakeholder vulnerability disclosure. ISO/IEC 29147:2018 and ISO/IEC 3011 may provide relevant guidance and recommendations. Cooperate with the private sector to: • foster cyber security by design • support private sector adoption of vulnerabilities management processes • coordinate sharing of vulnerability information • encourage bug bounty programmes, and • protect legitimate cybersecurity researchers and penetration testers.

Norm	Commentary on the norm	Examples of best-practice implementation of the norm by States
(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.	ICT activity in the context of this (and all the norms) is ICT activity with the potential to threaten international peace and stability. The global network of national CERTs provides essential services to the public, including incident response and cyber security advice. Cooperation among national CERTs is mutually beneficial and contributes to international peace and stability. Practical cooperation among CERTs must not be politicised. This norm recognises that CERTs should be protected from malicious cyber activity and, in turn, CERTs should not be used to conduct malicious activity. This norm encompasses activities conducted by the State itself. Further, the reference to "knowingly support" provides that States cannot evade the application of this norm by using proxies (see also paragraph 28(e) of the 2015 GGE Report).	Publicly reaffirm (for example in ministerial statements and policy documents) the commitment to act in accordance with all of the recommendations of the 2015 GGE Report, including this norm, and refrain from conduct in contravention of this norm. Establish an authorised national CERT. If a national CERT is not viable, designate a national cyber security point of contact. Ensure differentiation of national CERT functions from other functions of government. Foster strong relationships with industry and the technical community, in particular the CERT community (such as first.org. and APCERT), or with the national cyber security community where CERTs are not yet viable (for example: the Pacific Cyber Security Operators Network (PACSCON)).