Australian Government
Department of Foreign Affairs and Trade

Public Consultation: responsible state behaviour in cyberspace in the context of international security

Summary of public submissions on 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[i]), as endorsed by the UN General Assembly (A/RES/70/237[ii])

Australia's Department of Foreign Affairs and Trade conducted a public consultation process to inform Australia's engagement in the 6th UN Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security (GGE) and the inaugural UN Open Ended Working Group on Developments in the field of information and telecommunications in the context of international security (OEWG).

Below are verbatim excerpts from those public submissions which provided examples and suggestions of best practice implementation of one, some or all of the agreed norms of responsible state behaviour set out in the 2015 GGE report (A/70/174), as endorsed by the UN General Assembly (A/RES/70/237). Full versions of these submissions can be found on DFAT's website.[iii] The examples below represent the views of the organisations that submitted them and do not necessarily reflect the views of the Australian Government. Examples of Australian Government implementation of each norm can be found in Australia's OEWG Paper from September 2019.[iv] Commentary and examples of best practice implementation of the norms from Australia's representative to the GGE are also available on DFAT's website.[v]

Norm	**Examples of best practice implementation of the Norm**	
• 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:		
(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	Australian Strategic Policy Institute, International Cyber Policy Centre	• Implementation of norms are demonstrated by states' actions, capabilities, and strategic policy direction. As this norm deals with promoting inter-state cooperation on matters of international ICT security, examples of implementation include: - States' participation in cybersecurity forums as part of existing bilateral, multilateral or multi-stakeholder frameworks. Examples include political forums like ASEAN, ASEAN Regional Forum, East Asia Summit and the Pacific Island Forum; as well as technical and sectoral forums like ICANN, ISO, ITU and FIRST and INTERPOL, Freedom Online Coalition and the Bern Group for intelligence cooperation respectively. - States' (active) participation in the current OEWG and UNGGE, and/or their informal and intersessional meetings - States conducting bilateral, trilateral or multilateral cyber policy dialogues, like the Australia-Indonesia dialogue, or the Japan-ASEAN dialogue - States possessing operational capacities in the form of Ministries of Foreign Affairs and/or National Cybersecurity Agencies to engage in international cooperation and to be part of international dialogues - States' policy documents (like Australia's International Cyber Engagement Strategy), recorded interventions at the OEWG and/or statements by Cabinet ministers about matters of international cybersecurity.
	Global Partners Digital	• 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 humancentric 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.[vi] Furthermore, they are likely to include protections for strong technical standards for the protection of data, networks and infrastructure including strong encryption standards and comprehensive data protection legislation.[vii] 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.[viii]
	Institute for International Cyber Stability	• When malicious cyber incidents occur States should be willing to discuss publicly why the incident rose to the level of violating one of the 11 agreed UN GGE norms and specifically whether international law was breached. Tying specific incidents to specific norms and specific international rules will help clarify what the norms are and the law is as well as implement the 11 norms. This will also serve as a means to socialize or internationalize the norms.
	Kaspersky	• We believe that further development of clear industry standards, technical requirements and security measures applied to ICT products and services will help build cyber resilience globally. • Such standards and best practices have to be industry-led, consensus driven, interoperable and global to ensure they are applied consistently and universally. • A good example of such efforts is the Cybersecurity Act of the European Union, which prescribes the creation of the European Cybersecurity Certification Framework19 through a multistakeholder approach (namely, through a creation of Ad-Hoc Working Groups and the Stakeholder Cybersecurity Certification Group). • An additional example is the publication of draft guidelines on data protection 'by design' and 'by default' by the European Data Protection Board for a public consultation20. This illustrates how the concept and its technical and organizational measures have to be developed and applied according to industry's best practices and experience. Kaspersky has also shared its recommendations.[ix] • Greater transparency on Member States' activities in cyberspace and the rationale that informs their decision-making would reduce uncertainty and contribute to greater stability in cyberspace. In particular, it includes policy directives that outline priorities and intentions, strategy documents on ICT governance; ICT program budgets and roadmaps; descriptions of their initiatives to coordinate and cooperate with the community, including private sector, technical community, academia and civil society, on the beneficial use of ICTs.
	Microsoft	• In the wake of international ICT incidents, we encourage governments to explain how such actions violate international expectations for responsible behavior. Even coordinated attributions today often fail to explicitly connect the malicious activity with particular norms or international legal standards they have transgressed – including, for example, the Budapest Convention.
	Tech Accord	• First of all, governments should adopt and implement comprehensive national cybersecurity strategies, with the aim of increasing the resilience of their domestic online environment. Whenever possible these should incorporate an international cybersecurity strategy component. • Secondly, we encourage governments to adopt and make public their military doctrines, in particular as they relate to the online environment. • Thirdly, we encourage governments to establish, fund, and maintain Computer Emergency Response Teams (CERT) and ensure that they are able to coordinate, share good practice, and partner in response to an online incident. • Fourthly, we encourage governments to publish detailed statements explaining how they interpret the application of international law to cyberspace.

		• Finally, we encourage governments to participate in regional initiatives that aim to develop and implement confidence building measures, such as the work of the Organization for Security and Co-operation in Europe. Similarly, bilateral initiatives that aim to build trust between partners in cyberspace should be welcomed.
(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;	Australian Strategic Policy Institute, International Cyber Policy Centre	• Implementation of norms are demonstrated by states' actions, capabilities, and strategic policy direction. As this norm deals with means and methods to consider all relevant information in case of attributing an ICT incident, examples of implementation include: - States' practice of publishing regular cyber threat reports like Australia's Cyber Threat Report, Singapore's Cyber Landscape, Indonesia's HoneyNet project and The Netherlands' Cybersecurity Security Assessment. - States' use of frameworks like the UK's incident categorisation framework, Australia's governance framework for federal cyber crisis management, the US' impact assessment framework, and Singapore's response with a Commission of Inquiry following the SingHealth data breach - States' ability to follow a whole-of-government approach in reaching an informed position on an incident, i.e. having a process in place that links technical forensics with broader policy considerations. - States' ability to mobilise and deploy a variety of sources of national power across the spectrum of crisis response (prevention, diplomacy, incident management, and recovery), like the EU's Cyber Diplomacy Toolbox - States declaring policies and positions on attribution, like whether attributions will be made, publicly or privately, and how States will apply international law.
	Global Partners Digital	• 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.[x] 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.[xi] This contributes to uncertainty, supports deniability and can therefore make deterrence difficult. As a result, independent and trust-building attribution efforts are required.
	Institute for International Cyber Stability	• States should establish a clearing house type of information sharing center (fusion center) where the information from all stakeholders (cybersecurity firms, intelligence agencies, other government agencies with authorities to collect and analyse this type of data, civil society, academics) can be collected and analysed at the unclassified level. As states create such a center for national information sharing the government leaders can use this analyse to become more informed about ALL the relevant information in making attribution decisions.
	Kaspersky	• To overcome the lack of attribution or misattribution which can lead to escalation of tensions between states, it is necessary to develop transparent and trusted platforms for exchange of threat information between private actors and government agencies, including CERTs. • As an example of the private sector's approach, Kaspersky developed its Threat Intelligence Portal[xii] to provide access to technical descriptions of the very latest threats during an ongoing investigation; insight into non-public investigations; detailed supporting technical data and access to our YARA rules; continuous campaign monitoring; and access to actionable intelligence during an investigation (information on campaign distribution, IOCs, C&C infrastructure). As a support to cyber capacity building in the fight against cybercrime, we provide freemuim access to the Portal within our free package for Law Enforcement Agencies.[xiii]

	Microsoft	• To effectively consider all relevant information, including the larger context of the event etc., we recommend leveraging the resources, experience and expertise from all relevant stakeholders – including from industry and civil society/academia. This will enable states to develop the best possible big-picture understanding and situational awareness.
	Tech Accord	• First of all, governments should adopt a comprehensive incident response plan that prioritizes the mitigation of the incident. As part of the plan, relevant points of contact within government and critical infrastructures should be identified, and regular exercises should be conducted. Additional activities, such as e.g. staff exchanges could also be considered, assuming the necessary baseline level of trust has been built. • Secondly, governments should develop strategic and operational policies that inform their responses to cyber incidents, e.g. through military doctrine referenced above. Such transparency can increase predictability and promotes common understanding. • Thirdly, initiatives, such as the EU Cyber Diplomacy Toolbox can help make clear what are some of the responses that states can deploy as part of their response to an incident. • In particular it is important that diplomatic, economic, legal, and military options are all considered. • Fourthly, we welcome the fact that governments have begun sharing information and are becoming increasingly aligned in terms of attributing particular cyberattacks. We encourage governments to continue sharing the lessons learnt around different incidents. • Finally, the Cybersecurity Tech Accord signatories encourage governments to exchange information around particular cyberattacks with industry to ensure that the knowledge and situation awareness around a particular incident is as complete as possible.
(c) States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs	Australian Strategic Policy Institute, International Cyber Policy Centre	• Implementation of norms are demonstrated by states' actions, capabilities, and strategic policy direction. As this norm deals with a State's means and methods to prevent a its territory from being misused, examples of implementation include: - States' actions in combating common forms of cybercrime, such as phishing, spoofing, DDoS attacks. Other examples include practices of rules-based DNS filtering (for instance at ISP level) and seeking community reports (like Indonesia's patrolisiber.id). - such as Interpol ASEAN desk's operations with the Indonesian National Police. - States' ratification of the Budapest Convention or other international conventions addressing cyber and ICT-related crimes - States possessing operational cyber capacities in policing, law enforcement, counterintelligence and cyber defence - States' criminalisation of wrongful acts, including computer misuse, through specific cybercrime legislation, updated criminal codes, jurisprudence or police operational policies. - States' approach to combating cybercrime and enhancing security of the nation's cyber ecosystem, like the UK's Active Cyber Defence Program or government (loose) partnerships with ISPs and security researchers. - States declaring policy goals to combat transnational cybercrime, prevent terrorist use of the Internet and other potential wrongful acts, for instance in a national cybersecurity strategy or national cybercrime action plan.
	Global Partners Digital	• 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.[xiv] For example, where there has been misuse of personal data in political campaigns, companies should be investigated and brought to account.[xv] • 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".[xvi] 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).[xvii] • Due diligence is linked to the principle of state sovereignty. When applied to cyber operations, this principle would oblige a state to not knowingly allow its territory or the ICT infrastructure under its control to be used for cyber operations that affect the rights of other states. Because cyber operations can harm and infringe upon the human rights of individuals in other states makes the principle of due diligence imperative from a human rights perspective. Although it might be practically difficult to prove the "knowledge" element of this principle, as states can plausibly deny having actual or constructive knowledge of such activities, this does not render the legal obligation moot (see "Global Partners Digital, Unpacking the GGE's framework on responsible state behaviour: international law").
	Institute for International Cyber Stability	• This norm was not included in the section of the UN GGE 2015 report titled "How International Law Applies to the Use of ICTs" but rather in the section on "Norms, Rules and Principles." As such it is not clear whether all signing States agreed that this norms is based on international law. In order to increase the achievement of the implementation of this norm all States should first provide their position on whether this norms is based in international law. Assuming that some States' positions will be that it is not based in binding international law then in order to assist in the implementation of this non-binding norm States should codify domestic law that would criminalize any actions. Second, there should be an education campaign for States that need assistance in building the domestic legal framework for this while educating the prosecutors and judges. International sharing of information through a process like the MLATs needs to be instituted for investigations in order to gather the relevant information concerning the cases at issue. And lastly, each State should take reasonable steps to ensure that its own infrastructures are secure. This can be done by passing domestic regulation requiring a certain level of cybersecurity or by developing voluntary standards for cybersecurity such as the NIST standards in the US.
	Tech Accord	• First and foremost, states should develop comprehensive cybercrime laws to ensure that offences emanating from their territory can be prosecuted. Cybersecurity Tech Accord signatories would encourage state to leverage internationally established framework, such as the Budapest Convention on Cybercrime for this purpose. • Secondly, states should invest in capacity building for law enforcement and the judiciary to ensure that cybercriminals can be effectively prosecuted. • Thirdly, states should ensure that they are able to share and receive information surrounding a particular incident. In addition to recommendations outlined in the response to norm d), we encourage governments to ensure that their CERTs are part of international networks, such as the global Forum of Incident Response and Security Teams (FIRST) or similar initiatives. • Finally, states should promote cyber hygiene practices and thereby reduce the vulnerable attack surface. These could range from promoting patching, to adoption of Domain-based Message Authentication, Reporting & Conformance (DMARC), or Mutually Agreed Norms for Routing Security (MANRS).

(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;	Australian Strategic Policy Institute, International Cyber Policy Centre	• Implementation of norms are demonstrated by states' actions, capabilities, and strategic policy direction. As this norm deals with inter-state cooperation to stop cybercrime and terrorist use of ICTs, examples of implementation include: - States' use of existing law enforcement cooperation mechanisms, like mutual legal assistance treaties, to enable (joint) operations against cybercrime and cyber terrorism. - States' ability to use Interpol's and Europol's 24/7 cybercrime operations centres to assist operations and secure digital evidence - States establish dedicated cybercrime (police) units, like Dittipsiber (Indonesia), Anti-Cybercrime Group (Philippines) and Australian police forces' cybercrime units which can engage in transborder operations and information-sharing - States' active participation in Interpol, the UN open-ended intergovernmental expert group on cybercrime and the Global Internet Forum on Counterterrorism. - States' ability to provide and/or accept capacity building resources to enhance law enforcement in cybercrime. - States' ratification of the Budapest Convention and States' subscription to the Christchurch Call to Action.
	Global Partners Digital	• 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".[xviii]
	Kaspersky	• A greater cooperation with the community to fight cybercrime seems to us necessary. That includes greater threat information sharing, with the use of trusted communication channels, and greater cooperation on incident response with cybersecurity experts and private sector entities, technical community. • An example of such a public-private collaboration for information sharing could be the contribution agreement between INTERPOL and Kaspersky,[xix] signed in July 2019. Kaspersky pledged to provide human resources support, training, and threat intelligence data on the latest cybercriminal activities to INTERPOL, strengthening the organization's cyberthreat hunting capabilities.
	Microsoft	• Beyond inter-state cooperation, cooperative relationships should be built as necessary with members of the private sector as well as civil society and academia with access to relevant data, information and expertise to combat criminal activity online. For example, at Microsoft, the Digital Crimes Unit is responsible for coordinating with law enforcement around the globe to disrupt malicious criminal activities that interact with our infrastructure through actions including "botnet takedowns." • In addition, multistakeholder agreements, like the Christchurch Call to Eliminate Terrorist & Violent Extremist Content Online,[xx] can help set expectations and coordinate efforts across stakeholder groups to address dynamic challenges – including combatting extremist content online.
	Tech Accord	• Firstly, states should develop an overarching strategy for information sharing and collaboration domestically, and internationally. It should focus sharing on actionable threat, vulnerability, and mitigation information and prioritize voluntary information sharing. Information sharing should not only be limited to other states but it should also include the private sector. • Secondly, states should envision information sharing as a two-way process. If states are willing to share the information they have, their actions will demonstrate

		to their counterparts that they are indeed a partner in threat-information sharing, and help ensure that responders are focused on essential threats. • Thirdly, Information sharing should always be designed with privacy protections in mind. States should include strong privacy protections for the legitimate sharing, receipt and use of information in any cyber threat information sharing proposal. • Fourthly, on the international level, and as mentioned above, we believe the Council of Europe Convention on Cybercrime, i.e. the Budapest Convention, represents the most comprehensive and widely accepted international framework aimed at prosecuting the criminal use of ICT. We therefore urge states to adopt it and utilize its information sharing mechanisms to foster efficient information exchange. • Finally, multistakeholder agreements, like the Christchurch Call to Eliminate Terrorist & Violent Extremist Content Online, can help set expectations and coordinate efforts across stakeholder groups to address dynamic challenges – including combatting extremist content online.
(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;	Australian Strategic Policy Institute, International Cyber Policy Centre	• Implementation of norms are demonstrated by states' actions, capabilities, and strategic policy direction. As this norm deals with including respect for human and privacy, examples of implementation include: - States' support for civil society organisations that promote digital freedoms, domestically or internationally, like the Freedom Online Coalition or the Digital Defenders Partnership - States sponsoring or co-sponsoring relevant cyber and ICT-related resolutions at the UN Human Rights Council as a consequence of ratifying existing human rights conventions. - States' domestic framework that oversees and controls activities of law enforcement, defence, intelligence and other security agencies - States' privacy, data protections and human rights legislations, like the EU Global Data Protection Regulation; States endorsing principles like the right to be forgotten, and States entitling citizens access to public information (e.g. Indonesia's law on public information disclosure). - States' efforts to protect citizens (users), in particular vulnerable groups like children, indigenous people and elderly, in terms of e-safety. States assigning social and due diligence responsibilities to industries and internet services providers, like in the UK Online Harms paper. - States' efforts to provide relevant advice on e-safety and cybersecurity for human rights defenders, privacy watchdogs and whistle-blowers
	Global Partners Digital	• 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. • 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.[xxi] • 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).
	Institute for International Cyber Stability	• States should clarify what human rights they interpret to be part of binding international law. Where there is a common understanding on this then from that point a more specific and focused approach could be developed re human rights related to ICTs.
	Microsoft	• Considering the broader context, we recommend focusing on the promotion of common understandings of specific rules of international law, as outlined in our response to Question #4 below.[xxii]
	Tech Accord	• Cybersecurity Tech Accord signatories believe that the same rights that people have offline must also be protected online, and that this includes the right to freedom of expression and privacy. We urge states to ensure these are upheld, in line with their international commitments to human rights. • To this end, we encourage states to ensure human rights are at the heart of all their cybersecurity efforts, starting with national cybersecurity strategies, highlighted above. States should also consider institutionalizing offices charged with protecting human rights online, for example around online safety, information, or privacy. • Multistakeholder dialogue and engagement in pivotal in understanding how particular polices might impact the ability of individuals to exercise their human rights. With that in mind we urge states to consult with industry, and in particular with civil society, when adopting cybersecurity policies and approaches domestically; and engage with groups such as Freedom Online Coalition internationally.
(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	Australian Strategic Policy Institute, International Cyber Policy Centre	• Implementation of norms are demonstrated by states' actions, capabilities, and strategic policy direction. As this norm deals with the prohibition to damage critical infrastructure of other States, examples of implementation include: - States' acknowledgement of their sovereign cyber capabilities, including their mandate - States' sovereign cyber capabilities participate in national and international exercises - States develop, enact and publish operational policies or doctrines guiding their sovereign cyber capabilities - States make public statements on the application of international law and its commitment to upholding international obligations in the conduct of cyber operations - States provide transparency about the conduct and use of sovereign cyber capabilities.
	Global Partners Digital	• See recommendations with regards to critical infrastructure protection below.
	Institute for International Cyber Stability	• First, States should provide a list of what they consider to be critical infrastructure. Second, States should provide their interpretation of international law that focuses on the responses that would be lawful under international law if a State or its proxy were to violate this norm. Seeking a common understanding on what countermeasures under international law would be acceptable if critical infrastructure was intentionally damaged by a State or it proxy that has been attributed to a State would be very useful in the implementation of this norm.
	Microsoft	• We believe that the key step here will be to establish common standards — both technical and legal — for attributing internationally wrongful acts to states and

		to work towards defining a menu of lawful responses that could actually hold violators accountable while deterring others from undertaking similar acts, as outlined in our response to question #4 below.[xxiii]
	Tech Accord	• Firstly, it is clear that increased transparency around state activity online will help increase the stability and security of our common online environment. The Cybersecurity Tech Accord signatories therefore urge states to issue commitments that they will act in accordance with international law as well as norms of responsible state behavior agreed at the UN. • Secondly, we encourage states to go a step further and be transparent around how they interpret and implement international law and norms. This will not only help solidify these frameworks, but also allow other stakeholders to understand what cyber operations might be seen as permissible and which ones might draw consequences. • Thirdly, we urge states to adopt national critical infrastructure protection frameworks. This would not only serve to implement norm g (see below), but also increase transparency around what particular states consider critical infrastructure under their domestic frameworks. • Finally, we encourage states to develop effective accountability frameworks, which would allow perpetrators to be punished, and at the same time act as a deterrent against future violations.
(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;	Asia Pacific Network Information Centre	• There is work to do to define what entails critical infrastructure. Australia's submission to the UNOEWG process recognizes well this limitation. Something to consider is whether and how (g) also relates to the GCSC norm to protect the "public core". If the interpretation is that (g) could include elements such as packet routing and forwarding infrastructure, naming and numbering systems, cryptographic mechanisms of security and identity, etc.; then there is much that related Internet organizations can contribute as best practice implementation.
	Australian Strategic Policy Institute, International Cyber Policy Centre	• Implementation of norms are demonstrated by states' actions, capabilities, and strategic policy direction. As this norm deals with States' efforts to protect their own critical infrastructure, examples of implementation include: - States conduct a mapping of their critical national infrastructure, and critical information systems - States organise regular critical infrastructure incident exercises/drills and/or conduct (sectoral) cyber risk assessments - States invest in developing a qualified and skilled workforce - National cyber security centres or CERTs have the ability and mandate to support critical infrastructure sectors in case of incidents - States make best practice cyber security guidelines available, like the Australian Government's Information Security Manual. - States have legislation that describes cybersecurity responsibilities of critical infrastructure sectors in terms of information security and data protection, like the EU NIS Directive and GDPR, as well as Australia's Security of Critical Infrastructure Act and the Australian Energy Sector Cyber Security Framework (AESCSF), and Indonesia's 2019 implementing regulation (no. 71) in respect to the 2012 Law of Information and Electronic Transactions law.
	Global Partners Digital	• 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.[xxiv] 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.[xxv] • 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.[xxvi] 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.
	ICRC & Australian Red Cross	• While cyber security and defence are constantly improving, older systems with outdated or even non-existent cyber security are particularly vulnerable to cyber attacks and will remain a concern in the years to come. Both the public and private sectors have a role to play through industry standards and legal regulation.[xxvii] • In the health-care sector, for instance, the regulatory environment should be adapted to the increased risk, such as through standardisation requirements, with a view to ensuring resilience in the event of a cyber attack. Cyber security needs to be taken into account in the design and development of medical devices and networks and updated throughout their lifetime, no matter how long they last. Similarly, for industrial control systems, industry standards, whether imposed or self-imposed, are critical. This includes reporting incidents and sharing information between trusted partners.[xxviii] • In terms of IHL, parties to armed conflicts must take all feasible precautions to protect civilians and civilian objects under their control against the effects of attack. This is one of the few IHL obligations that States must already implement in peacetime, especially with regard to fixed installations. While cyberspace is a virtual global domain, the obligation to take precautions against the effects of attacks extends at least to the physical infrastructure of cyberspace (and to objects whose functioning depends on that infrastructure) located in a State's territory, or in any territory that may be occupied by a party to the conflict.[xxix] • Among many other avenues that could be explored,[xxx] States could consider creating a "digital watermark" to identify certain actors or infrastructure in cyber space that must be protected (such as objects that enjoy specific protection under IHL). The aim would be to help their identification and prevent them from being targeted during armed conflicts. The potentially positive effects in terms of protection against unintended harm by law-abiding actors would however need to be balanced against the risk of disclosing information on critical infrastructure to potential adversaries, including criminals. The prospects of positive effects might depend in part on attribution becoming easier.[xxxi]
	Institute for International Cyber Stability	• States should develop domestic plans and policies for critical infrastructure cybersecurity (i.e., US Commerce Department, NIST Cybersecurity Framework). States should also invest in training of relevant stakeholders in the different sectors of critical infrastructure.
	Kaspersky	• To address the rapid development of emerging technologies and the resulting changing threat landscape that has the potential to impact the critical infrastructure protection, we suggest the following actions: - a government-industry supply chain security task force to identify best practices, guidelines and lessons learned for secure technology procurement, and evaluation of ICT suppliers' trustworthiness; - transparency vulnerability management programs to ensure the integrity of critical infrastructure by ensuring operators can fix vulnerabilities before they are exploited by hostile actors; and

		- private-to-government (including government-to-government and private-to-private) threat information sharing about cybersecurity threats, vulnerabilities, and incidents, including with affected parties and companies capable of developing means to develop remediation plans against attacks. • Among existing legal instruments to address critical infrastructure protection, we would like to highlight the EU Security of Networks and Information Systems (NIS) Directive,[xxxii] which has produced sector cybersecurity guidance and developed a framework to support the assessment of cyber-resilience of regulated organizations (i.e., operators of critical infrastructure and digital service providers). In 2018, the UK[xxxiii] also implemented the NIS Directive after a public consultation to collect proposals from private actors on introducing the cross-sector Critical National Infrastructure (CNI) regulation. • In particular, we highly welcome several aspects of the NIS Directive such as establishing cooperation of CERTs, rules, procedures and thresholds for incident response as well as transparent reporting requirements.
	Microsoft	• To ensure that organizations that provide critical infrastructure and services are prepared to manage cyber threats as they increasingly use digital technologies, we recommend that states foster the adoption of cyber risk management best practices and security baselines. As further described in a white paper[xxxiv] and by a global, cross-sector industry coalition,[xxxv] it is critical that such practices and baselines be interoperable across regions and sectors, leveraging best practices like ISO/IEC 27103[xxxvi] or the NIST Cybersecurity Framework[xxxvii] and promoting continuity and understanding across highly integrated supply chains and operations.
	Tech Accord	• Cybersecurity Tech Accord signatories have been encouraged by the increased focus by states around the world on protecting critical infrastructure and services from online threats. We urge states to continue focusing in this space and to: - Establish comprehensive policies and plans for protecting critical infrastructure, based on risk management best practices; - Foster capabilities for preventing, detecting, responding to, and recovering from risks to promote operational resiliency. - Promote innovation and investments by learning from policy and operations that can guide the allocation of resources for practices, programs, education, and research related to critical infrastructure protection. • Furthermore, we encourage state to leverage established security baseline approaches, such as ISO/IEC 27103[xxxviii] or the NIST Cybersecurity Framework,[xxxix] to ensure that frameworks are interoperable across regions and sectors, as well as promote continuity and understanding across highly integrated supply chains and operations. • As mentioned above, sharing information around what entities have been designed as critical infrastructure would act as an effective confidence building measure. • Finally, we encourage states to invest in capacity building efforts domestically in this space, organizing workshops and trainings with key stakeholders responsible for protecting critical infrastructures from online threats.
(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	Asia Pacific Network Information Centre	• APNIC ran a workshop[xl] at the IGF in 2019 where this norm was discussed. There were several interventions that raised questions about who exactly would issue and respond to such a request. The technical community pointed out that in many instances these requests would not naturally loop into the national CERT, sectorial CERTs or other governmental actors. Formalizing these requests could potentially introduce a level of latency that could undermine rather than support cyber security practitioners to resolve an incident.
	Australian Strategic Policy Institute,	• Implementation of norms are demonstrated by states' actions, capabilities, and strategic policy direction. As this norm deals with States' ability and willingness to respond to requests for assistance, examples of implementation include:

malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty;	International Cyber Policy Centre	- States' participation in regional points of contact schemes, like the ASEAN cyber points of contact directory - States facilitate a 24/7 cybersecurity information exchange mechanism - States' cybersecurity agencies participate in multilateral policy networks, networks of CERTs and networks of international police forces. - States have an ability and willingness to provide and accept (technical) assistance with incident and crisis management, for example through a deployable assistance team or existing support arrangements like the Pacific Cyber Security Operators Network (PacSON). - States' endorsement of the recommended confidence-building measures from the 2015 UNGGE report, like the set of cyber confidence building measures adopted by the OSCE or the Sydney Recommendations on Practical Futures for Cyber Confidence Building in the ASEAN region.
	Global Partners Digital	• 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"[xli] and the EU's "Directive on security of network and information systems".[xlii]
	Institute for International Cyber Stability	• Clarity on the principle of due diligence under international law would be especially helpful in implementing this norm. It is generally accepted that under the principle of due diligence in international law if a State is requested to help in investigating some harmful activity emanating from that State, the State being requested should assist in that request. A number of States have also supported the position that this principles of international law requires a State to take specific steps to mitigate any malicious ICT activity emanating from its territory. States should seek consensus on the due diligence principle under the law and provide their positions in writing regarding how the principle applies to the use of ICTs.
	Microsoft	• In responding to and dealing with such requests, and where appropriate, we recommend leveraging the resources, experience and expertise from all relevant stakeholders – including from industry and civil society/academia. All of these actors can act as "force-multipliers" for each other, thereby creating a situation where the joint effort is larger than the sum of its parts.
	Tech Accord	• Firstly, to implement the norm, states should ensure that the appropriate points of contact are identified, kept up to date, and have sufficient resources to be able to respond to any incoming requests. Cybersecurity Tech Accord signatories believe that taking a leaf from coordinated vulnerability disclosure, states should also have communication plans in place and ensure that they respond to the request even if it is determined that they are unable to help. • Secondly, in responding to with such requests, and where appropriate, we recommend leveraging the resources, experience and expertise from all relevant stakeholders, including from industry and civil society. • Thirdly, states should participate in information sharing initiatives, either at regional level or bilaterally, which ensure that contacts and trust is established well before a specific incident can occur. • Finally, as highlighted above under norms c, state should have comprehensive frameworks in place that allow them to prosecute actors active on their territory. Cybersecurity Tech Accord signatories believe that the principle of due diligence forms a key aspect of international law and that creates an additional duty to mitigate malicious ICT activity in this context.
(i) States should take reasonable steps to ensure the integrity of the supply chain so that end users can	Australian Strategic Policy Institute, International	• Implementation of norms are demonstrated by states' actions, capabilities, and strategic policy direction. As this norm deals with States' efforts to ensure the integrity of the ICT supply chain, examples of implementation include: - States issue guidance on risk management in the ICT supply chain

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;	Cyber Policy Centre	- States conduct a national telecommunications supply chain review, like the UK in 2019 - States introduce an IT security certification scheme like the UK's Cyber Essentials; and States' participation in international arrangements for mutual recognition of certified products and service, like the Common Criteria initiative - States' prohibiting the deliberate introduction of systemic weaknesses/vulnerabilities in ICT products; and States combating black markets in ICT products. - States' participation in the Wassenaar Arrangement on the transparency of dual-use goods and technologies - States have national bodies technically able and mandated to advice, assess and certify industry products and consumer goods, like a national cybersecurity centre, universities of national scientific organisations. - States' emerging practice of considering ICT products and services as critical national (security) infrastructure, like the decisions of various States in regard to 5G infrastructure providers or cybersecurity service providers. - States' ability to access Industry transparency centres, like Huawei's centre in the UK, Microsoft's in Singapore, and Kaspersky's in Switzerland.
	Global Partners Digital	• 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.[xliii] 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.[xliv] • Other steps states can take to support supply chain integrity include the conduct of human rights impact assessments[xlv] 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).[xlvi]
	ICRC & Australian Red Cross	• Those who develop cyber capabilities should consider creating obstacles to make repurposing difficult and expensive. While it is hardly possible from a technical standpoint to guarantee that malware cannot be repurposed, methods like encrypting its payload and including obstacles in different components of the code, for example, could raise the bar in terms of the expertise required to reengineer malicious tools.[xlvii]
	Kaspersky	• Supply chain attacks remain the most destructive and difficult to prevent. Therefore, for the implementation of this norm is crucial to develop frameworks for technical and institutional evaluation of the trustworthiness of supply chain vendors. From the vendor side, it is important to ensure the integrity of the supply chain through the publicly communicated policies and practices. Our Global Transparency Initiative[xlviii] (GTI) as a set of practical measures to increase transparency and accountability in cybersecurity could be a guiding example for the private sector. • Practically speaking, the GTI includes framework to build trust and confidence of users in cybersecurity: - **Data Care**: relocation of data processing and data storage to Switzerland – a state with long famous neutrality and strict data protection regulation; - **Dedicated Transparency Centers**[xlix] for accessing Kaspersky's source code, software updates and threat detection rules, along with other activities, for external review. There we also provide access to review types of information

		which, in general, Kaspersky products send to our cloud-based Kaspersky Security Network (KSN); and rebuild the source code to make sure it corresponds to publicly available modules. Our Transparency Centers are located in Zurich and Madrid and will soon be launched in Kuala Lumpur and São Paulo. Because of the pandemic, we are launching the remote access to some of the options for executive briefings provided at our Transparency Centers; - **Secure and reliable engineering practices** confirmed through third-party independent assessments, including the SOC 2 audit by a 'Big Four' accountancy firm[i] and ISO 27001 certification (to be publicly announced in February 2020); - **Vulnerability Management Program**: responsible cooperation with security researchers and a Bug Bounty Program with awards of up to $100k for the most critical flaws found in Kaspersky's systems. - To support capacity building for greater resilience to supply chain risks, Kaspersky launches its **Cyber Capacity Building Program** with dedicated training on product security evaluation to help companies, government organizations and academia to develop mechanisms to secure their ICT infrastructure. The training course would be available both online and offline and will include sections on source code review, threat modelling and vulnerability management. • Among industry-led initiatives addressing supply chain security, we would like to highlight the Software Trustworthiness Best Practices[ii] recently published by Industrial Internet Consortium. There Kaspersky shared its view on non-technical aspects that should be within the scope while measuring user trust in software. • There are some public sector-led best practices aimed at ensuring the security of supply chains in the IoT, and where Kaspersky was invited to participate: 1) the UK Consumer IoT Security Code of Practice[iii] - which was the basis of the ETSI TS 103 645 standard; and 2) ENISA's annual studies for the Good Practices for Security of IoT – Secure Software Development Lifecycle.[iiii] • These examples illustrate cooperative work to address existing gaps in software development, and we believe that this format with industry's engagement in producing guidelines and best practices for addressing supply chain risks has to be applied further.
	Microsoft	• We encourage states to take a holistic approach to supply chain risk management, working to help all stakeholders mitigate risks to security and integrity not just at the procurement stage but also through strong internal controls, such as those related to configuration management, segregation of duties, change management, and access management. More broadly, states can help all stakeholders develop and implement effective approaches to supply chain risk management, which require understanding the lifecycle of threats and then applying a combination of policy, technical controls, operational controls, and vendor and personnel controls in a risk-based manner.
	Tech Accord	• A foundational principle of the Cybersecurity Tech Accord is that its signatories will protect against tampering with and exploitation of technology products and services during their development, design, distribution and use. We strongly support this norm and encourage states to publicly commit to uphold it, including when it comes to considerations of weakening encryption or mandatory key escrow. • The Cybersecurity Tech Accord was partly created to stand for cybersecurity and in opposition to the emergence of an industry focused on selling vulnerabilities and surveillance technologies. We encourage states to not encourage those practices and to proactively seek to prohibit them. • We also encourage states to participate in the Wassenaar Agreement, which regulates transfers of dual used goods and technologies with military applications. However, we also urge states to consider more regular consultations with the industry when it comes to inclusion of new technologies into this framework.

		• Finally, we urge states to take a holistic approach to supply chain risk management, working to help all stakeholders mitigate risks to security and integrity not just at the procurement stage but also through strong internal controls, such as those related to configuration management, segregation of duties, change management, and access management. Moreover, given that supply chains regularly span multiple countries states should actively promote and encourage other states in securing their parts of the supply chain. This could be done by regular state-to-state dialogues but also by encouraging information exchange and capacity building in the private sector.
(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;	Australian Strategic Policy Institute, International Cyber Policy Centre	• Implementation of norms are demonstrated by states' actions, capabilities, and strategic policy direction. As this norm deals with States' efforts to encourage responsible reporting of ICT vulnerabilities, examples of implementation include: - States acknowledge and endorse public vulnerability reporting policies for, and by, government and non-governmental organisations - States accept the practice of legitimate bug bounty programmes engaging private sectors, cyber security industry and security researchers - States establish a vulnerability equities processes that guides decision-making by their sovereign cyber capabilities - States endorse relevant ISO standards and, for instance, the GFCE global good practises on CVD. - States provide adequate legal provisions to support, encourage and protect responsible reporters. - States organise hacking sessions, like Indonesia's "Everybody can hack" or the US' "Hack the Pentagon" competition.
	Global Partners Digital	• 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 stakeholders with regards to vulnerability reporting,[liv] 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[lv] and should codify government disclosure processes into law to ensure compliance.[lvi] • In addition, states should set up coordinated vulnerability disclosure processes,[lvii] to engage all stakeholders in vulnerability reporting, in accordance with the guidelines and recommendations defined in ISO/IEC 29147:2014 and ISO/IEC 3011.[lviii] • 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.[lix] • 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",[lx] and "bug bounty programmes".[lxi] States should also fund defensive vulnerability discovery and research and invest in building security researcher communities.
	ICRC & Australian Red Cross	• The preferred option for enhancing the safety of cyber space should be disclosing vulnerabilities to the appropriate software developer or vendor so that the vulnerabilities can be fixed.[lxii] In this regard, we welcome the fact that the Australian Signals Directorate (ASD) has adopted Responsible Release Principles for Cyber

		Security Vulnerabilities[lxiii] that take as their starting position to disclose weaknesses found. The risks entailed by a decision not to disclose vulnerabilities in view of the specific characteristics of cyber space should be duly considered in these kinds of decision-making frameworks.
	Institute for International Cyber Stability	• States should develop their domestic process for vulnerability disclosure for their own country. For example, see the US Vulnerabilities Equities Process at the White House. If many States were to develop such a process then it would be possible for States to share the information gained from this process re remedies at the global level.
	Kaspersky	• The norm should address both the creating of coordinated vulnerability handling and mitigation processes where Member States can intake vulnerability reports from external researchers with regard to state networks and systems and thus contribute to enhancing their security and resilience. • The norm could also be operationalized through developing vulnerability equities processes by Member States (as suggested by the Global Commission on the Stability of Cyberspace[lxiv]), and coordinated vulnerability disclosure programs by non-state actors. • In this regard, we highly welcome the developing efforts of several states to establish transparent policies for responsible vulnerability disclosure (for instance, policies that are set up by Australia,[lxv] the Netherlands[lxvi]), and bug bounty program running together with a third party (for instance the UK NCSC Bug Bounty Program[lxvii] at HackerOne or the Bug Bounty Program run by the Government Technology Agency (GovTech) and Cyber Security Agency (CSA) of Singapore[lxviii]). • We at Kaspersky run our program for transparent coordinated vulnerability disclosure called Vulnerability Report[lxix] as well as our Bug Bounty Program together with HackerOne mentioned above. • We have recently also developed our Ethical Principles for Responsible Vulnerability Disclosure that have been inspired by guidelines from FIRST. We believe that the entire ICT ecosystem would be more secure, if other players make their vulnerability disclosure approaches transparent. • As multistakeholder best practices, we would like to highlight the following: - In 2018, Kaspersky also took part in the study[lxx] by the Centre for Policy Studies (CEPS) under the chairmanship of Ms. Schaake – a former member of the European Parliament. Within a working group with other companies we discussed challenges to software CVD in Europe and as an outcome prepared practical recommendations to address existing challenges. - In 2020, Kaspersky took part in the UNIDIR Workshop dedicated to operationalizing cyber norms, where it was widely discussed and agreed that risks of legal proceedings and lack of transparent policies with trusted communication channels are often key challenges to the greater security of products and applications available on the market. To address that, we at Kaspersky joined the Dislose.io[lxxi] project to offer a safe harbor for security researchers – we pledged not to initiate legal proceedings against those who look to research our products and find vulnerabilities in there.
	Microsoft	• We encourage states to each adopt and publish respective Vulnerabilities Equities Processes (VEP), detailing how they evaluate whether to retain or disclose information on a potential ICT vulnerability, with a default position to always disclose to vendors to develop a fix and improve the security of the ICT ecosystem. Examples: - UK Equities Process[lxxii] - USA VEP[lxxiii]
	Tech Accord	• Cybersecurity Tech Accord signatories believe that vulnerability management policies represent a key tool in increasing the stability of our online environment. With that in mind, we have encouraged our signatories to adopt these policies and make them available here.[lxxiv] We urge states to similarly encourage adoption of vulnerability management across their local ecosystems. Whilst large ICT vendors

		typically have these in place, this is not necessarily true for smaller entities, or companies that are new to developing technology solutions (e.g. car manufacturers or banks). • Secondly, we encourage states themselves to require all departments to establish vulnerability disclosure policies, with clear processes and safe havens for security researchers, as the United States has recently embarked upon. • Thirdly, states should ensure that the legal frameworks they have in place allow security researchers to find and report vulnerabilities without negative sanctions for their behavior. • Finally, we encourage states to each adopt and publish respective Vulnerabilities Equities Processes, detailing how they evaluate whether to retain or disclose information on a potential ICT vulnerability. Cybersecurity Tech Accord signatories believe these should: - Presume disclosure as the starting point; - Mandate that all government-held vulnerabilities, irrespective of where or how they have been identified, go through an evaluation process leading to a decision to disclose or retain it; - Make public the criteria used in determining whether to disclose a vulnerability or not. In addition to assessing the relevance of the vulnerability to national security, these criteria should also consider threat and impact, impact on international partners, and commercial concerns; - Clearly consider the impact on the computing ecosystem if the vulnerability is released publicly and the costs associated with cleanup and mitigation; - Ensure any decision to retain a vulnerability is subject to a six-month review; - Ensure that any retained vulnerabilities are secure from theft (or loss).
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.	Asia Pacific Network Information Centre	• APNIC ran a workshop[lxxv] at the IGF in 2017 where this norm was discussed. As pointed out in different submissions, Microsoft and GPD, it is important to establish collaboration mechanisms with industry and the technical community, in particular the CERT community via first.org.
	Australian Strategic Policy Institute, International Cyber Policy Centre	• Implementation of norms are demonstrated by states' actions, capabilities, and strategic policy direction. As this norm deals with States' efforts to refrain from harming recognised CERTs, examples of implementation include: - States establish and assign an authorised national CERT - Participation of authorised national CERTs in regional and international networks, like FIRST, APCERT, OIC-CERT, PacSON - Participation of authorised national CERTs in international cybersecurity exercises and challenges, like the ASEAN Cyber Incident Drill. - States ensure a separation of roles and responsibilities of the authorised national CERT from other arms of government - States make public statements and commitments to the legal and legitimate use of sovereign cyber capabilities, and its adherence to international law and the norms.
	Global Partners Digital	• 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.[lxxvi] • 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.[lxxvii]
	Institute for International Cyber Stability	• States should articulate what level of harm that this norm is focused on. International law already prohibits action by one State within the territory of another State (whether this is harm against the government, private sector like critical infrastructure or a combination like a CERT may be) that rises to a certain level of harm (i.e., a use of force). In developing clarity on what level of harm this norm is prohibiting then it may be grounded in or another of international legal principles. This would improve the likelihood of this norm being implemented. This would also serve to deter those States that violate this norm since the victim State would be allowed to conducted responses to the violator therefore raising the costs to those States that chose to violate this norm. • States should pass domestic law or policy that identifies CERTs as critical infrastructure.
	Microsoft	• We believe that digital activities central to daily life deserve protection from cyberattacks. The GGE and the OEWG can and should declare that everyday activities — such as access to food, water, energy, housing, mass transit and other transportation infrastructure, basic functions of civil government (e.g., voting, issuing licenses), health care, and core elements needed for the internet itself to function — should be off-limits to cyberattacks by governments and non-governmental actors. Such declarations would contribute to a process of building expectations and rules governing cyberspace.
	Tech Accord	• As with norm f), we believe that increased transparency around state activity online will help increase the stability and security of our common online environment. The Cybersecurity Tech Accord signatories therefore urge states to issue commitments that they will act in accordance with international law as well as norms of responsible state behavior agreed at the UN. • Secondly, we encourage states to go a step further and be transparent around how they interpret and implement international law and norms. This will not only help solidify these frameworks, but also allow other stakeholders to understand what cyber operations might be seen as permissible and which ones might draw consequences. • Finally, we encourage states to develop effective accountability frameworks, which would allow perpetrators to be punished, and at the same time act as a deterrent against future violations.

[i] https://dfat.gov.au/international-relations/themes/cyber-affairs/Documents/ungge-2015-a70174.pdf
[ii] https://dfat.gov.au/international-relations/themes/cyber-affairs/Documents/ungge-2015-a-res-70-237.pdf
[iii] https://www.dfat.gov.au/international-relations/themes/cyber-affairs/Pages/public-consultation-responsible-state-behaviour-in-cyberspace-in-the-context-of-international-security-at-the-united-nation
[iv] https://www.dfat.gov.au/sites/default/files/how-australia-implements-the-ungge-norms.pdf
[v] https://www.dfat.gov.au/international-relations/themes/cyber-affairs/Pages/international-security-and-cyberspace
[vi] 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.
[vii] Association of Progressive Communications and Global Partners Digital, "Unpacking the GGE's framework on responsible state behaviour: Cyber norms"
[viii] Ibid
[ix] https://edpb.europa.eu/sites/edpb/files/webform/public_consultation_reply/kasperskys_submission_on_the_guidelines_on_article_25_data_protection_by_design_and _by_default.pdf
[x] Association of Progressive Communications and Global Partners Digital, *"Unpacking the GGE's framework on responsible state behaviour: Cyber norms"*
[xi] Egloff, Florian J. (2019) *"Contested public attributions of cyber incidents and the role of academia"*

[xii] https://opentip.kaspersky.com/

[xiii] https://media.kaspersky.com/en/enterprise-security/supporting-law-enforcement-agencies.pdf

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

[xv] Information Commissioner's Office (ICO) *"Investigation into data analytics for political purposes"*

[xvi] 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

[xvii] Ibid

[xviii] *Open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime*

[xix] https://www.kaspersky.com/about/press-releases/2019_kaspersky-extends-cooperation-with-interpol-in-joint-fight-against-cybercrime

[xx] https://www.christchurchcall.com/

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

[xxii] https://www.dfat.gov.au/sites/default/files/cyber-submission-microsoft.pdf

[xxiii] https://www.dfat.gov.au/sites/default/files/cyber-submission-microsoft.pdf

[xxiv] GFCE, *"Global Good Practices - Critical Information Infrastructure Protection";* the GFCEMERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers; Companion Document to the GFCE-MERIDIAN Guide on CIIP

[xxv] GFCE, Companion Document to the GFCE-MERIDIAN Guide on CIIP

[xxvi] OECD (2019) "*Recommendation on Digital Security of Critical Activities"*

[xxvii] ICRC, *'The potential human cost of cyber operations'* (L. Gisel and L. Olejnik, eds), Expert Meeting Report (*'Human Cost Report'*), May 2019, p9

[xxviii] *Human Cost Report* pp 9 and 39-40.

[xxix] Position Paper, p. 6; ICRC, *'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts',* October 2015, p. 43; https://www.icrc.org/en/download/file/15061/32ic-report-on-ihl-and-challenges-of-armed-conflicts.pdf.

[xxx] *Human Cost Report,* pp. 39-42 and 75-77.

[xxxi] *Human Cost Report,* pp. 9 and 40 - 41.

[xxxii] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

[xxxiii] https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018

[xxxiv] http://download.microsoft.com/download/4/6/0/46041159-48FB-464A-B92A-80A2E30B78F3/MS-riskmanagement-securitybaselines-WEB.pdf

[xxxv] https://www.crx2.org/

[xxxvi] https://www.iso.org/standard/72437.html

[xxxvii] https://www.nist.gov/cyberframework

[xxxviii] https://www.iso.org/standard/72437.html

[xxxix] https://www.nist.gov/cyberframework

[xl] https://www.intgovforum.org/multilingual/content/igf-2019-—-day-3-—-saal-europa-—-ws-63-usual-suspects-questioning-the-cybernorm-making

[xli] OECD (2019) *"Recommendation on Digital Security of Critical Activities",*

[xlii] European Commission, *"The Directive on security of network and information systems (NIS Directive)"*

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

[xliv] Internet Society, Online Trust Alliance

[xlv] Article 19, *"Assessing the Human Rights Impact of Internet Registries"*

[xlvi] 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

[xlvii] *Human Cost Report,* p. 9.

[xlviii] https://www.kaspersky.com/transparency-center

[xlix] https://www.kaspersky.com/transparency-center-offices

[l] https://www.kaspersky.com/about/compliance-soc2

[li] https://www.iiconsortium.org/pdf/Software_Trustworthiness_Best_Practices_Whitepaper_2020_03_23.pdf

[lii] https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security

[liii] https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1

[liv] 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)"*

[lv] 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

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

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

[lviii] 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

[lix] 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"*

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

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

[lxii] *Human Cost Report,* pp. 9 and 33-34.

[lxiii] https://www.asd.gov.au/publications/Responsible-Release-Principles-for-Cyber-Security-Vulnerabilities

[lxiv] https://cyberstability.org/norms/#toggle-id-5

[lxv] https://www.cyber.gov.au/tags/security-vulnerability

[lxvi] https://english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline

[lxvii] https://hackerone.com/ncsc_uk

[lxviii] https://www.csa.gov.sg/news/press-releases/second-government-bug-bounty-programme-expanded-to-cover-more-systems-and-digital-services

[lxix] https://support.kaspersky.com/general/vulnerability

[lxx] https://www.ceps.eu/ceps-publications/software-vulnerability-disclosure-europe-technology-policies-and-legal-challenges/

[lxxi] https://www.kaspersky.com/blog/kaspersky-joins-disclose-io/27588/

[lxxii] https://www.gchq.gov.uk/information/equities-process

[lxxiii] https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF

[lxxiv] https://cybertechaccord.org/vulnerability-disclosure-policies/

[lxxv] https://www.intgovforum.org/multilingual/content/igf-2017-day-3-room-xi-ws38-international-cooperation-between-certs-ws38-technical-diplomacy

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

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