Cybersecurity Tech Accord submission to Australian consultation on:
Responsible state behavior in cyberspace

The Cybersecurity Tech Accord signatories are grateful to the Australian government, and in particular to the Department of Foreign Affairs and Trade (DFAT), for the opportunity to provide our input into the Australian consultation around the two United Nations (UN) processes focused on responsible state behavior in cyberspace: the Open-Ended Working Group (OEWG) and the Governmental Group of Experts (GGE). We welcome the work in these two bodies, as regardless of target, cyberattacks increasingly impact the security of civilians and the stability of international relations.

The Cybersecurity Tech Accord is a public commitment of over 140 companies to promote a safer online world by fostering collaboration among global technology companies committed to protecting their customers and users and helping them defend against malicious threats. We believe that by combining the resources and expertise of the global technology industry, we can create a starting point for dialogue, discovery and decisive action to more effectively:

- Provide our customers, users and the developer ecosystem with information and tools that enable them to understand current and future threats and better protect themselves.
- Protect our customers and users everywhere by designing, developing and delivering products and services that prioritize security, privacy, integrity and reliability, and in turn reduce the likelihood, frequency, exploitability and severity of vulnerabilities.
- Work with each other and likeminded groups to enhance cybersecurity best practices, such as improving technical collaboration, coordinated vulnerability disclosure and threat sharing, as well as ensuring flexible responses for the wider global technology ecosystem.
- Oppose efforts to attack citizens and enterprises by protecting against exploitation of technology products and services during their development, design, distribution and use.

While the Cybersecurity Tech Accord signatories are pleased that the UN continues to engage on this important topic, both through the relevant Group of Governmental Experts (GGE), Open-Ended Working Group (OEWG), and the implementation of the recommendations of the High-Level Panel on Digital Cooperation, there are limited opportunities available for non-governmental stakeholders to be able to put their views forward and we have called for greater inclusion of these previously[1]. While states clearly have a leading role to play in creating and upholding a normative framework for behavior, the multistakeholder community must also play a pivotal role in providing input and helping set direction for these discussions as they relate to cyberspace. With this in mind, the Australian initiative to hear from other interested stakeholders is particularly praiseworthy, and we hope will be emulated by other countries in the future.

We have also been heartened by the UN Intersessional meeting in December, where we were honored to be able to highlight our views on confidence building measures in particular[2], building on our work and

[1] Call for inclusion of additional voices in international debates on responsible nation state behavior in cyberspace: https://cybertechaccord.org/call-for-inclusion-of-multi-stakeholders-in-international-debates-on-responsible-nation-state-behavior-in-cyberspace/

[2] Cybersecurity Tech Accord joins the UN dialogue to limit the offensive use of digital technologies: https://cybertechaccord.org/cybersecurity-tech-accord-joins-the-un-dialogue-to-limit-the-offensive-use-of-digital-technologies/

contributions to responsible state behavior in cyberspace over the past year. This included submissions to the UN High Level Panel on Digital Cooperation,[3] to the Organization of American States on confidence building measures[4], and the Internet Governance Forum's Best Practice Forum on Cybersecurity[5], as well as work on the Paris Call for Trust and Security in Cyberspace[6] and the Report of the Global Commission on Stability of Cyberspace[7]. Across these documents, the following high-level recommendations remained constant:

- Implement and uphold international norms: International norms of responsible behavior in cyberspace are fundamental to creating a common understanding of acceptable and unacceptable actions. Of course, and here we are in complete agreement with the Australian government, the international community must now take concrete action to uphold the norms that have already been agreed.
- Develop confidence-building measures: In tandem with emerging international norms of behavior and increased transparency, confidence-building measures (CBMs) are an effective way to contribute to peace and stability in cyberspace, by way of increasing the understanding of intent behind particular actions. Given their potential role in the de-escalation of hostilities, the international community would be well served by agreeing to and implementing a discrete set of CBMs.
- Consider and include multi-stakeholder efforts: As highlighted above, there is room for improvement when it comes to including more voices into the UN discussions. One way to rectify that is to incorporate the outcomes of widely accepted multistakeholder efforts, such as the Paris Call for Trust and Security in Cyberspace[8], which currently has over 1,000 supporters and includes the Australian government, into the final documents.
- Exercise restraint: Overall, as tensions around the world increasingly include an online dimension, the Cybersecurity Tech Accord signatories call on the international community to exercise restraint. We are especially concerned by the outsized impact cyberattacks can have on civilians and civilian institutions. It is critical that all stakeholders recognize that a stable and trustworthy cyberspace remains in the best interest of the international community.

Taking these as a baseline, we provide more detailed answers to the questions posed in the next section of our submission. We hope the responses provide a helpful contribution in advancing a shared objective: achieving a rules-based and rights-respecting online world for all. The Cybersecurity Tech Accord looks forward to subsequent opportunities to work together and provide further input on issues related to cybersecurity. Should you have any questions that emerge based on our input, please do not hesitate to contact us.

[3] Submission to High Level Panel on Digital Cooperation: https://cybertechaccord.org/uploads/prod/2018/12/Tech-Accord-HLP-Response-Dec-2018.pdf

[4] Promoting international peace and stability by building trust between states in cyberspace: The importance of effective confidence-building measures : https://cybertechaccord.org/uploads/prod/2019/04/FINALOASWP.pdf

[5] Best Practices Forum on Cybersecurity Culture, Norms and Values: https://cybertechaccord.org/best-practices-forum-working-group-on-cybersecurity-culture-norms-and-values-cybersecurity-tech-accord-response-to-a-call-for-contributions/

[6] Paris Call on Trust and Security endorsement: https://cybertechaccord.org/endorses_paris_call/

[7] Global Commission on enhancing stability in cyberspace https://cybertechaccord.org/the-cybersecurity-tech-accord-welcomes-the-global-commissions-singapore-norm-package-offers-comments-on-enhancing-stability-in-cyberspace/

[8] https://pariscall.international/en/

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

The Cybersecurity Tech Accord signatories welcome the fact that both the UN processes start with an effort to understand the cyberthreat landscape today. We believe that up-to-date information on sophisticated threats needs to be a point of departure for any discussion on how to increase the stability of cyberspace. Having said that, it is important to remember that today's advanced threat actors, including state and non-state entities, continue to adapt their tactics based on a variety of factors, including shifts in opportunity, digital infrastructure, and geopolitical conditions. Modern cyberthreats have also evolved to include a broad range of objectives, including cybercrime, information warfare, espionage, etc.

Keeping this continuous evolution in mind, combined with the pace of technological innovation, we would suggest the Australian government does not necessarily focus on a specific threat as part of the upcoming discussions. This approach could limit and constrain governments to a view of the threat landscape at a specific point in time, which is unlikely to serve the global community well over time. Moreover, given the different levels of technological adoption and cybersecurity readiness amongst the UN member states, the cyberthreats they face will continue to vary. We would therefore recommend focusing on end goals (e.g. cyber-bullying) rather on specific means how that might be accomplished (e.g. specific social platform or sexting).

Instead, we encourage the Australian government to champion regular interactions with cybersecurity experts, across the private industry and in academia, to ensure the awareness of the latest developments and trends remains current. For example, Australia could commit to partner with technology providers to host a yearly workshop on the topic on the margins of First Committee the meetings, or this could become a regular commitment for the Committee itself.

Moreover, we encourage trainings or briefings that are tailored to a particular member state to be made available under the capacity building frameworks. This will allow countries to not only understand how to secure their current online environment, but to understand the latest trends and learn about good practices others are, or have, considered.

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

As mentioned at the onset of this contribution, the Cybersecurity Tech Accord signatories are grateful for the opportunity to provide feedback to this consultation, and also to have been able to participate at the Intersessional meeting in December. We are hopeful that the multistakeholder community will be able to participate more regularly in some of these meetings, in particular the OEWG. Whilst we acknowledge the primary role governments play in this context, we firmly believe that a multistakeholder dialogue is critical for us to collectively being able to find a path forward on what are sometimes challenging and thorny issues.

The private industry develops, owns and maintains a significant majority of the global ICT infrastructure, and as a result we have a special responsibility to help ensure its safe and secure use globally. It is the industry that knows the ins and outs and technology, and as such it should be involved to share experiences and insights on threats, as well as possible solutions. Moreover, the speed of technological development means that the environment we operate in changes every few months, if not weeks. A formal regular dialogue, including a consultation process and briefings on these issues, would ensure that the options governments are discussing are sufficiently future proof and not designed to solve for problems that have been left on the scrapheap of innovation.

Furthermore, it is pivotal that the fact that these discussions are taking place, as well as their importance to the technology industry, are made better known. Not nearly enough industry and civil society entities are familiar with the UN dialogues. We are proud to have been able to introduce a new set of industry representatives to this debate, and we are committed to doing so in the future. We strongly encourage the Australian government to publicize their efforts further, to both domestic and international audiences.

It is also important that these discussions are made more accessible, in particular to entities from emerging economies, both from civil society and industry. Webcasting the OEWG discussion is a welcome step forward, however we would also encourage governments to create a stipend to bring new discussants to the conversation, as well as also potentially utilizing regional organizations to consult with the local communities ahead of meetings at the UN.

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

First of all, the Cybersecurity Tech Accord signatories wish to thank the Australian government for its leadership in detailing its position on international law and cyberspace, first in 2017, and then elaborating it further last year. We believe statements like this help reinforce existing agreements, clarify potential ambiguities, and begin the process of building a common interpretation of international law for cyberspace. We were delighted to also see France, UK, the Netherlands, and others also begin on this path. We hope that other countries will heed the invitation highlighted in the GGE mandate and follow suit.

In a similar vein, the Cybersecurity Tech Accord signatories would like to see the UN processes reaffirm the agreements reached in the 2013 and 2015 UN GGEs, by restating that international law applies to cyberspace, as well as highlighting the importance of international humanitarian law in this regard, and the fact that human rights need to be upheld offline as well as online. Upholding these values, irrespective of the debates that might emerge around how particular rules are to be implemented, is in our view, critical to long-term stability.

Nevertheless, the Cybersecurity Tech Accord signatories are concerned that established international frameworks aren't enough to prevent some of the most egregious acts in cyberspace. This relates not just to questions of interpretation, but the fact that there are limited tools available to hold perpetrators accountable. Public shaming of certain perpetrators, a step that taken by an increasing number of states in recent years, including Australia, is praiseworthy. However, we urge governments to be even more detailed in their condemnations and highlight, even retrospectively, which laws the actions have broken. Furthermore, we encourage government to make public, again retrospectively if necessary, as much information as possible that led to their decision to attribute a particular attack to a particular actor. Making that data available to the research community in particular would substantially increase the trust in those statements.

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

No other area under consideration by the OEWG and UNGGE has the potential to make as large an impact on the security and stability of cyberspace as the promotion of cybersecurity capacity building. International law, norms, and confidence building measures can only be implemented and adhered to if member states have the capability and capacity to act on them. However, even with increased attention supply continues to fall short of what is needed and efforts are often uncoordinated, both internationally and within countries. Given the limited resources available, as well as the nature of the online environment, well-coordinated international efforts are critical to ensuring a common level of resilience and understanding across the globe.

Instead of replicating any existing efforts, the Cybersecurity Tech Accord signatories encourage member states to pool resources to generate greater impact, and participate in fora, such as the Global Forum for Cyber Expertise (GFCE), which can act as match-making mechanisms between the needs and expertise. Furthermore, we recommend that through a concerted targeted effort is started to bring the industry more fully into these discussions. There are numerous trainings already available, in particularly focused on the technical aspects of cybersecurity, and we believe these could be leveraged to a much greater extent.

We believe that this latter effort will also make it easier to keep abreast of the latest trends in technology and maintain the relevance of capacity building. Any capacity building needs to seek to both address the current need, but also to empower the receiving stakeholders to leapfrog their counterparts by learning from them. Even more importantly, capacity building needs to be treated as a continuous process, rather than a series of one-off engagement.

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

While recognition of the applicability of the international law, as well as the agreements reached in the 2013 and 2015 GGE reports, represent great progress, the Cybersecurity Tech Accord signatories believe it is now time to discuss the "how". With that in mind, we recommend that Australia argues for the UN to recognize that more needs to be done. Some of the recent trends have demonstrated that international law does not sufficiently prohibit some of the most egregious and unwanted cyberactivity, and also that even when a particular activity is prohibited, the law is not consistently applied and therefore oftentimes ineffective. It would therefore be beneficial if *all* UN member states were encouraged to produce official positions on how international law applies in cyberspace to clarify respective positions and drive towards consensus. Similarly, we recommend that states highlight, in line with the examples set by Australia and Canada, how they are implementing individual norms and report back on progress made on an annual basis.

Moreover, a number of multistakeholder initiatives have put forward recommendations on new norms and principles in recent years. The primary amongst these, and to which the Cybersecurity Tech Accord companies are a proud signatory, is the Paris Call for Trust and Security in Cyberspace. With that in mind, we would recommend incorporating the following the principles agreed in that forum into the UN dialogues:

- "Prevent malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities;"
- "Prevent ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sector;" and

- "Prevent activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet."

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

The Cybersecurity Tech Accord signatories in particular welcome the Australian government's focus on practical implementation of the agreed norms of behavior. Indeed, we hope that the examples set by the Australian and Canadian government, which shared the overviews of their efforts so far in this space, will be emulated by others. To that end, we propose that a mechanism is established as part of the OEWG or GGE that would encourage governments to report on their progress on an annual basis. It is our view that this will not only add more pressure on governments to act, but will also help solidify the acceptance of agreed upon norms. Finally, we believe that that a database of collated activity would also significantly advance capacity building efforts.

In the table below, the Cybersecurity Tech Accord signatories provide a set of high-level recommendations as to how individual norms could be implemented. We hope that the Australian government will continue on this path and consult on each of the individual norms in the future, creating an opportunity to develop a compendium of concrete good practices and standards that states could leverage in their norms implementation, again importantly aiding capacity building work.

2015 GGE consensus report norms and implementation recommendations:

GGE consensus report (2015) (¶13)	Recommendation
(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.	▪ 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;	▪ 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;	▪ 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	▪ 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.

whether new measures need to be developed in this respect;	▪ 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;	▪ 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;	▪ 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;	▪ 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 or the NIST Cybersecurity Framework, 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 malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty;	▪ 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 have confidence in the security of ICT products. States should seek to prevent the proliferation of	▪ 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.

malicious ICT tools and techniques and the use of harmful hidden functions;	▪ 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;	▪ 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. 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: o Presume disclosure as the starting point; o 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; o 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; o Clearly consider the impact on the computing ecosystem if the vulnerability is released publicly and the costs associated with cleanup and mitigation; o Ensure any decision to retain a vulnerability is subject to a six-month review; o 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	▪ 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.