Microsoft Corporation Tel 425 882 8080
One Microsoft Way Fax 425 936 7329
Redmond, WA 98052-6399 http://www.microsoft.com/

Microsoft

Microsoft's contribution to Australia's engagement in the United Nations' dialogues on information security

Microsoft would like to thank the Australian government, and the Department of Foreign Affairs and Trade (DFAT) specifically, for the opportunity to provide input into the ongoing dialogues at the United Nations (UN) focused on improving the safety and stability of cyberspace – the Group of Governmental Experts (GGE) and the Open Ended Working Group (OEWG). While respectful of the unique responsibility governments have in matters of national security, the inherently shared nature of cyberspace requires collaboration between and across stakeholder groups to protect the safety and integrity of the online world. To that end, we appreciate Australia's continuing efforts to seek out and include the perspectives from the private sector in particular in these matters. We hope the responses below to the questions provided by DFAT are useful as these dialogues continue, and stand ready to provide additional clarifications, as required.

For further information on Microsoft's priorities related to these matters, we encourage you to consult our recent position paper submitted to the UN Office of Disarmament Affairs (UNODA) (2019), as well as our contribution to the Internet Governance Forum's Best Practice Forum (BPF) on Cybersecurity (2019) focused on norms implementation. Links to both papers are below.

Position paper to UNODA: https://www.un.org/disarmament/wp-content/uploads/2019/12/protecting-people-in-cyberspace-december-2019.pdf

BPF Contribution: https://www.intgovforum.org/multilingual/filedepot_download/8396/1723

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

Microsoft has unique insights into the constantly evolving threat environment online based on the work of our security teams, which track the malicious activities of some of the most sophisticated actors in cyberspace. Today's advanced threat actors, including both 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. At the same time, emerging technological trends, such as improved artificial intelligence (AI), the proliferation of internet-of-things (IoT), and increased global connectivity, have significantly expanded the attack surface exploited by malicious actors, as well as their capabilities. As new attack vectors have broadened the risk profile for all users, several prominent trends are worth highlighting:

Geopolitical objectives

- Critical infrastructure targets. Threat actors regard critical infrastructure as a target for attack, jeopardizing the civilian populations which rely on them. State actors have successfully disabled public access to electricity in rival countries, and have reportedly targeted adversaries' power grids by implanting malware as a latent threat that can be triggered at their discretion.[1]

[1] Greenberg, Andy. *How Not To Prevent a Cyberwar With Russia.* Wired. June 18, 2019. https://www.wired.com/story/russia-cyberwar-escalation-power-grid/

Microsoft Corporation Tel 425 882 8080
One Microsoft Way Fax 425 936 7329
Redmond, WA 98052-6399 http://www.microsoft.com/

- Disinformation campaigns. State actors have attempted to undermine democratic processes and manipulate public discourse through information operations, notably by leveraging social media. Coordinated attempts to use internet-enabled interference to influence the outcome of elections or undermine trust in democratic institutions and processes was observed, *inter alia*, in the 2016 United States presidential elections, the 2017 French elections, and elsewhere.

Financial gain

- Crypto-mining. The number of attacks aiming to generate cryptocurrency by using compromised systems to divert computing power has been rapidly increasing. While these attacks can often fly below the radar, and are not meant to be destructive *per se*, they nonetheless degrade computer performance, waste electricity, and create a foothold in a system for other malicious activities.[2] Moreover, compromised systems existing on cloud infrastructure can generate additional computing costs for the owner.
- Ransomware. These attacks lock users out of their computer systems until they pay a "ransom," and continue to be a weapon of choice for financially-motivated threat actors. These attacks disproportionately impact vulnerable entities that fail to update their systems or invest in redundancies.[3] Recent examples include high-profile attacks on US municipalities, including the cities of Baltimore and Atlanta, as well as the global "WannaCry" attack in 2017.

Methods employed

- Automation and AI. State tactics are rapidly changing, in line with technological developments. For example, as AI improves, through advances in machine learning and neural networks, it will be used for cyber offense not just defense. Moreover, AI could be used to propagate misinformation, particularly through synthetic media. In addition, intellectual property tied to developing AI systems makes it a prime target for malicious actors seeking financial gain or commercial advantage in this rapidly-growing space.
- DNS hijacking. Recent years have also seen attackers taking advantage of, and corrupting, the underlying infrastructure of the Internet through, for example, DNS hijacking. This approach sees attackers manipulate and redirect Internet traffic to funnel victims into an attacker-controlled environment for exploitation.[4] High profile DNS hijacking attacks have been leveraged against Wikileaks, and the New York Times.[5]
- Internet of Things. The proliferation of IoT also poses new challenges, as threat actors gain the ability to leverage the computing power of large numbers of infected devices. The rapid growth and pervasive deployment of these devices has meant that these are frequently vulnerable due to insecure configuration. These attacks are often an entry point into associated networks to enable other malicious activity.[6]

---

[2] *Microsoft Security Intelligence Report, Volume 24, January-December 2018*. Microsoft. https://info.microsoft.com/SIRv24Report.html

[3] *Microsoft Security Intelligence Report, Volume 24, January-December 2018*. Microsoft. https://info.microsoft.com/SIRv24Report.html

[4] *DNS Infrastructure Hijacking Campaign*. Dept. of Homeland Security – Cybersecurity and Infrastructure Security Agency. Jan 11, 2019. https://www.us-cert.gov/ncas/current-activity/2019/01/10/DNS-Infrastructure-Hijacking-Campaign

[5] Greenberg, Andy. Hacker Lexicon: What Is DNS Hijacking?. Wired. Sept. 4, 2017. https://www.wired.com/story/what-is-dns-hijacking/

[6] *Corporate IoT – a path to intrusion*. Microsoft Security Response Center. August 5, 2019. https://msrc-blog.microsoft.com/2019/08/05/corporate-iot-a-path-to-intrusion/

Microsoft Corporation Tel 425 882 8080
One Microsoft Way Fax 425 936 7329
Redmond, WA 98052-6399 http://www.microsoft.com/

- Military-to-military. While offensive cyber capabilities have been around for a while, they are now becoming more integrated within traditional military operations. Recent examples have included the publicly acknowledged cyberattacks by the US military in its campaign against ISIS.[7]
- Phishing and spearphishing. Phishing continues to be the preeminent attack method for threat actors and will likely continue to be a major problem as it preys on human judgement in response to evolving and creative attacker *lures*. Modern phishing attacks leverage multiple web addresses and public cloud infrastructure to avoid detection. While phishing attacks can have a broad range of objectives, spearphishing attacks, by contrast, are targeted, usually involving more sophisticated spoofing campaigns with an objective of credential stealing, espionage or intrusion.[8]
- Spying-as-a-service. There is increasingly a formalized economy of independent third-party entities selling spyware and other malicious services to governments and others for the purposes of spying on targets domestically and abroad. Third party services offer customizable tools exploiting zero-day vulnerabilities[9], advanced surveillance software[10], and may even offer on-demand cyber-offensive operations.

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

Microsoft agrees wholeheartedly with Australia that the so-called "Framework for Responsible State Behavior in Cyberspace" (the Framework) – comprised of the 2010, 2013 and 2015 GGE consensus reports – lays an important foundation for protecting and maintaining a safe, secure, and rights-respecting online world. By recognizing the authority of international law in cyberspace, as well as defining a set of norms for responsible state behavior, the Framework goes a long way to establishing clear expectations in the digital domain. However, it is equally clear that the contents of this Framework have been insufficient thus far to prevent the escalating numbers of sophisticated cyberattacks we see today.

There are also important new norms and principles that should be considered to clarify expectations for responsible state behavior and to keep pace with the evolving nature of cyber threats. While the GGE process has not delivered a consensus report since 2015, forums outside the UN have nevertheless advanced the discussion on cyber norms in the years since and should be looked to for guidance to enhance the Framework. With that in mind, and if Australia agrees, we would encourage the GGE and OEWG to explore the following ways to strengthen existing UN norms and establish necessary additional norms:

[Note: input on international law and capacity building are addressed in later questions]

Strengthen existing norms:

[7] In Fight Against ISIS, U.S. Adds Cyber Tools. NPR's Weekend Edition. February 28, 2016 https://www.npr.org/2016/02/28/468446138/in-fight-against-isis-u-s-adds-cyber-tools

[8] *Microsoft Security Intelligence Report, Volume 24, January-December 2018*. https://info.microsoft.com/SIRv24Report.html

[9] Gambrell, Jon. *U.A.E. Cyber Firm DarkMatter Slowly Steps Out of the Shadows.* Bloomberg. Jan 31, 2018. https://www.bloomberg.com/news/articles/2018-02-01/uae-cyber-firm-darkmatter-slowly-steps-out-of-the-shadows

[10] Diebert, Ron, Bill Marczak, John Scott-Railton, Adam Senft, Bahr Abdul Razzak. *The Kingdom Came to Canada*. The Citizen Lab. Oct 2018. https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/

Microsoft Corporation Tel 425 882 8080
One Microsoft Way Fax 425 936 7329
Redmond, WA 98052-6399 http://www.microsoft.com/

- Affirm 2015 GGE norms. The current GGE and the OEWG should reaffirm the validity and authority of all 11 norms recognized in the 2015 GGE report, in their entirety. They should also explain what the implementation of these norms is expected to look like to improve state compliance.
- From voluntary to binding. To further strengthen the 2015 norms, both UN bodies should strive to turn these politically-binding commitments into legally-binding rules. Such efforts should be based on the premise that a) existing international law applies to cyberspace, and b) any new instrument that is developed would need to be consistent with, and operate in support of, international human rights law [including freedom of expression and the right to privacy].

Agree on necessary new norms:

States and other actors continue to innovate and evolve in their methods and their targets. In line with that, norms of behavior for cyberspace must also continue to adapt. Two recent processes offer valuable multistakeholder recommendations in this space:

- Adopt additional Paris Call norms. Given the widespread, global, multistakeholder support for the nine principles included in the *Paris Call for Trust and Security in Cyberspace*, the UN dialogues should recognize the 3 principles included in the agreement that were not reflected in earlier GGE reports, and adopt them as additional norms. These are:
    - "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."
- Adopt GCSC norms. We also encourage Australia to support the recognition by the GGE and OEWG of the 8 norms introduced by the Global Commission for the Stability of Cyberspace (GCSC),[11] which include expectations for both state and non-state actors:
    - State and non-state actors should not conduct or knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace.
    - State and non-state actors must not pursue, support or allow cyber operations intended to disrupt the technical infrastructure essential to elections, referenda or plebiscites.
    - State and non-state actors should not tamper with products and services in development and production, nor allow them to be tampered with, if doing so may substantially impair the stability of cyberspace.
    - State and non-state actors should not commandeer others' ICT resources for use as botnets or for similar purposes.

[11] *Rules of the Road: GCSC Proposed Norms for Rules of the Road in Cyberspace*. Global Commission on the Stability of Cyberspace (GCSC) https://cyberstability.org/norms

Microsoft Corporation Tel 425 882 8080
One Microsoft Way Fax 425 936 7329
Redmond, WA 98052-6399 http://www.microsoft.com/

- States should create procedurally transparent frameworks to assess whether and when to disclose not publicly known vulnerabilities or flaws they are aware of in information systems and technologies. The default presumption should be in favor of disclosure.
- Developers and producers of products and services on which the stability of cyberspace depends should prioritize security and stability, take reasonable steps to ensure that their products or services are free from significant vulnerabilities, take measures to timely mitigate vulnerabilities that are later discovered and to be transparent about their process. All actors have a duty to share information on vulnerabilities in order to help prevent or mitigate malicious cyber activity.
- States should enact appropriate measures, including laws and regulations, to ensure basic cyber hygiene.
- Non-state actors should not engage in offensive cyber operations and state actors should prevent or respond to such activities if they occur.

3. As stated above, a key Australian objective is for the OEWG and/or GGE to provide practical guidance on observation and implementation of the agreed norms of responsible state behaviour, set out in the 2015 GGE report [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 11 voluntary norms laid out in the 2015 consensus GGE report focus exclusively on state responsibilities, and so in some cases fall beyond the purview of guidance Microsoft can provide as a private company. However, we feel there are certainly best practices and effective policy approaches for implementing respective norms, as well as opportunities for further collaboration across stakeholder groups in support of the 11 norms (a-k), which we have highlighted below.

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.	• 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.
(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;	• 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

Microsoft Corporation Tel 425 882 8080
One Microsoft Way Fax 425 936 7329
Redmond, WA 98052-6399 http://www.microsoft.com/

	enable states to develop the best possible big-picture understanding and situational awareness.
(c) States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;	
(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;	• 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, 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;	• 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.
(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;	• 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.

Microsoft Corporation Tel 425 882 8080
One Microsoft Way Fax 425 936 7329
Redmond, WA 98052-6399 http://www.microsoft.com/

(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;	• 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 and by a global, cross-sector industry coalition, it is critical that such practices and baselines be interoperable across regions and sectors, leveraging best practices like ISO/IEC 27103 or the NIST Cybersecurity Framework and promoting continuity and understanding across highly integrated supply chains and operations.
(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;	• 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.
(i) States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions;	• 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.
(j) States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies	• We encourage states to each adopt and publish respective Vulnerabilities Equities Processes (VEP), detailing how they evaluate

Microsoft Corporation Tel 425 882 8080
One Microsoft Way Fax 425 936 7329
Redmond, WA 98052-6399 http://www.microsoft.com/

to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure;	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 ○ USA VEP
(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	• 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.

4. The mandate of the GGE invites members to annex to the GGE report "*national contributions…on the subject of how international law applies to the use of information and communications technologies by States*". Through the International Cyber Engagement Strategy, Australia has published its positions on the application of international law to cyberspace in 2017 and 2019 [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?

After reviewing Australia's position statements related to international law from 2017 and 2019, we deeply appreciate the thoughtful analysis provided and feel well aligned with the government's perspective and vision for cyberspace as an environment where state conduct is governed by the rule of law. The 2013 and 2015 UN GGE reports indeed make clear that international law does apply to state cyber operations, to include: the law regarding the use of force; International humanitarian law (IHL); International human rights law; The law of State responsibility; and the duty of non-intervention. Indeed, we believe such a rules-based order to be essential for the security and stability of the global public internet upon which people everywhere depend.

We appreciate as well the breadth and depth of Australia's statements on its own government's interpretation of existing international law and how it applies to state conduct in cyberspace, and join in encouraging governments everywhere to similarly release statements of their own to help "deepen understandings and set

Microsoft Corporation Tel 425 882 8080
One Microsoft Way Fax 425 936 7329
Redmond, WA 98052-6399 http://www.microsoft.com/

clear expectations"[12] in a domain where too much ambiguity still persists. We believe such efforts can go a long way to promote common understandings, highlight where there are disagreements, and reduce the risk of misunderstandings with potentially unintended consequences.

However, in addition to affirming that international law does indeed apply in cyberspace and that states should be encouraged to reflect upon and share how they interpret its application, Microsoft feels there are still important gaps and grey areas in international law as it relates to cyberspace that need to be addressed. The current cybersecurity dialogues at the UN present a valuable opportunity to address these thorny issues. In particular, we have identified five discrete challenges when it comes to applying international law to ICTs.

1) Existential disputes: Some states insist that certain existing areas and principles of international law – such as *self-defense, international humanitarian law*, and *due diligence* – are not applicable to cyberspace operations.

2) Interpretative disputes: Even where states agree an international legal concept applies to cyberspace, they may disagree on what it means. With respect to sovereignty, for example, some states view it as a "rule" that a state's cyber-operations can violate directly. Others insist it is a background "principle" that informs the content of other rules (e.g., the duty of non-intervention), but does not (yet) directly constrain state behavior.

3) Application clarity: Aside from the GGE reports and statements referenced above, states have largely remained silent on how international law applies to cyber operations generally, and have largely refrained from invoking it or claiming violations in specific cases.

4) The enforcement problem: International law has limited tools available for holding states who violate it accountable for their actions. For example, international law may limit states' ability to respond collectively to an attack, so if a cyber operation against one state violates international law it is unclear if a collection of states would be allowed to respond and how. Some have called for revisions to international law that would accommodate collective counter-measures, but the broader question of what enforcement is possible in this space remains. Without appropriate enforcement tools, international law may not actually deter unwanted state cyber operations.

5) The effectiveness gap: Even if states agreed on whether and how international law applies to state cyber operations, existing law still may permit some of the most egregious behavior. In other words, there is a "gap" between the conditions of stability and responsibility the law would like to achieve and what its contents actually require. For example, international law does not directly prohibit systemic cyber operations targeting individuals short of the use of force. Nor does international law do much to regulate foreign "influence operations" targeting electoral processes. Moreover, the amount of control a state must exert over non-state actors to be legally responsible for their behavior grants sophisticated states a "grey zone" in which they can "encourage" activity they could not legally conduct themselves. As such, new international laws may be required to bridge this effectiveness gap to ensure international law fulfils the functions for which it exists in the first place.

We believe addressing the gaps and challenges in international law identified above is essential to establishing a digital ecosystem where obligations and expectations for responsible state behavior are both recognized and respected. Indeed, it can be difficult to reconcile legal standards intended for a physical domain with cyberspace. And yet, this clarity is essential for pushing back against dangerous trends in the weaponization of the online world, where ambiguity is too often exploited to reckless ends that can jeopardize individuals and

[12] *2019 – Supplement to Australia's Position on the Application of International Law in Cyberspace.* Department of Foreign Affairs and Trade, Australia. 2019. https://dfat.gov.au/international-relations/themes/cyber-affairs/Documents/application-of-international-law-to-cyberspace.pdf

Microsoft Corporation Tel 425 882 8080
One Microsoft Way Fax 425 936 7329
Redmond, WA 98052-6399 http://www.microsoft.com/

organizations as readily as conventional weapons. The following are discrete recommendations for how to the GGE and OEWG may work to address the "grey areas" in international law:

- Reaffirm commitments. The 2013 and 2015 GGE reports made important contributions to the availability and application of international law to the cyber domain. Further progress made in either the current GGE or OWEG must be based on first reaffirming the authority of international law, including IHL, in cyberspace.
- Confirm existing international law regimes apply to cyber operations. Microsoft encourages the current UN cyber dialogues to reaffirm international law's application to cyberspace generally, including the rights of states granted by the UN Charter. This application of international law specifically includes:
    - International Humanitarian Law (IHL) which includes the qualification that even cyber operations targeting only data can be considered "attacks" to which its various principles -distinction, proportionality, necessity – still apply; and
    - Due diligence holding a state liable for transboundary harms caused by malicious cyber activities originating in its territory of which it had advance warning or about which it reasonably should have been aware.
- Promote common understandings of specific rules of international law. Microsoft encourages the UN dialogues to agree on common understandings of how international law operates in cyberspace, across:
    - The UN Charter's prohibition on the use of force/armed attacks – including (i) whether cyber-operations alone may trigger the use of force prohibition, and (ii) what standard states should employ to delimit when the use of force or right to self-defense is crossed;
    - Sovereignty – including recognizing it as a rule that state cyber operations should not violate, but which must also be consistent with international human rights law. Notably, while Australia's statements on international law in cyberspace do mention this as a key challenge, they stop short of articulating whether and how "sovereignty" regulates state cyber-operations separate from—and in addition to—the regimes on the use of force and non-intervention.;
    - The duty of non-intervention – including which ICT networks or infrastructure comprise the *domain reservé* in which states must not intervene, and what cyber operations qualify as "coercive" for purposes of triggering the prohibition;
    - State responsibility – including what level of "control" a state must have over a non-state actor to be deemed liable for its activities; and
    - Human Rights – including the need to protect freedom of speech without facilitating violent on-line extremist behavior.
- Recognize that existing international law is presently insufficient and ineffective. Given current trends, it is clear that international law either (a) does not sufficiently prohibit some of the most egregious and unwanted cyber activity, including systemic cyber-operations targeting individual users or their infrastructure below the use of force threshold, or (b) provides a "patchwork" of contested rules (and meanings) resulting in insufficient and/or ineffective regulation of the unwanted activity.
- Encourage increased transparency by states. Following Australia's example, it would 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. These steps will help improve certainty and predictability about future behavior in cyberspace and how international law applies.
- Promote efforts to hold states accountable for violating international law. Microsoft encourages the current UN cyber dialogues to establish common standards – both technical and legal – for attributing

Microsoft Corporation Tel 425 882 8080
One Microsoft Way Fax 425 936 7329
Redmond, WA 98052-6399 http://www.microsoft.com/

internationally wrongful acts to states and a menu of lawful responses that could actually hold violators accountable while deterring others from undertaking similar acts.

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

Both the OEWG and the GGE have the potential to positively impact the security and stability of cyberspace by joining in promoting cybersecurity capacity building. After all, cybersecurity norms and confidence building measures can only be effective if states have the capabilities and capacities to implement them. Even beyond the structures of the United Nations, there are important steps that countries with advanced cyber capabilities like Australia can take, and indeed are taking, on their own to promote capacity building across the digital divide. These actions include supporting awareness raising campaigns and initiatives, as well as contributing to independent institutions capable of effectively matching capacity building needs with quality resources and expertise. Microsoft continues to support such efforts as well, both independently and through associations like the Cybersecurity Tech Accord, to provide necessary industry guidance to ensure capacity building programs meaningfully address cybersecurity challenges.

Microsoft encourages the OEWG and GGE, as well as countries in positions to support bilateral and regional capacity building initiatives, to promote and support the following:

Utilize existing mechanisms. Numerous states, foundations, and private actors have already dedicated funding and resources to capacity building initiatives that have become increasingly effective and well-coordinated in recent years. Instead of replicating those efforts, Microsoft encourages Member States to pool resources to generate greater impact, and participate actively and on a persistent basis in fora, such as the *Global Forum for Cyber Expertise*, which can help match needs with expertise and bring necessary stakeholders together. The OEWG and GGE could help strengthen these efforts by not only calling for further capacity building in consensus reports, but also explicitly recognizing the leading organizations working to successfully coordinate these efforts today.

Understand the need. Capacity building efforts can only succeed if they are responding in a targeted way to a real need. They therefore need to begin with participants' understanding of what issues matter to them and why, as well as with an understanding of where they have gaps in capacity or capability. Inevitably, these needs will vary depending on regional or local context. Recognition of this dynamic would be welcome guidance to include in any reports developed by either the OEWG or GGE.

Strengthen cyber diplomacy. All too often, capacity building efforts focus on the technical aspects of cybersecurity, which are necessary but insufficient. One area that would benefit from additional capacity building attention and resources is efforts to strengthen cyber diplomacy capabilities in countries around the world. This would help to ensure that all Member States are equipped to participate in relevant international negotiations on a more equal footing. The inclusive nature of the OEWG process highlights the importance of precisely this kind of capacity building, so all states are able to effectively advocate for their citizens on cybersecurity issues that impact all nations..

Be inclusive of all stakeholders. It is critical that capacity building focuses not just on government stakeholders, but industry and civil society as well. Moreover, effective cybersecurity capacity building programs also rely on the support of government stakeholders as well as industry and civil society organizations with relevant expertise to develop trainings, exercises, and other initiatives. This essential multistakeholder dynamic in

Microsoft Corporation Tel 425 882 8080
One Microsoft Way Fax 425 936 7329
Redmond, WA 98052-6399 http://www.microsoft.com/

capacity building – in both delivering and receiving – should therefore be recognized in any guidance produced on the subject by the OEWG or GGE.

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

Microsoft is encouraged by the growing recognition of the need for more formalized and enduring multistakeholder participation in dialogues on cybersecurity rules and in the institutions that reinforce them, at the UN and beyond. This includes the participation of the private sector, which must take greater responsibility for both complying with and establishing international expectations for responsible behavior in cyberspace, as the owners and operators of the majority of its infrastructure. We are optimistic as well about the important work NGOs are doing, on an apolitical basis, to promote accountability to cybersecurity norms in particular – this includes the work of the CyberPeace Institute, which Microsoft partnered in founding this past fall, as well as other groups committed to accountability and transparency, like The Citizen Lab at the University of Toronto. Academia also needs to continue to play an indispensable role in promoting greater understanding of past ICT incidents and the implications of existing international law and norms.

In the context of the current UN discussions, Microsoft recommends the following objectives and would welcome Australia's support in advancing them:

- Facilitate multistakeholder inclusion. Institutional dialogue that creates a consistent, meaningful role for industry, academia, and civil society participation – alongside governments and other institutions – is critical. The development of norms and rules will benefit significantly from a multistakeholder approach as dialogue restricted to government participants does not reflect the input or expertise of communities that directly manage ICTs or that have experience advocating for peace and security across a range of contexts and issues.

  The decision to include a multistakeholder community during the December intersessional meeting of the OEWG was a significant step forward in this regard, and we appreciate as well the regional multistakeholder consultations of the GGE. However, multistakeholder inclusion in these dialogues continues to be ad-hoc, limiting the potential benefits of regularized ongoing collaboration. To this end, establishing a formal consultative process for the GGE, and a formal participation structure for the multistakeholder community in the OEWG, would be to the benefit of both dialogues.

- Formalize institutional dialogues. The UN can facilitate progress by sustaining multistakeholder dialogue, though conversations should not be constrained to a single venue. Progress can and should be made across different forums and institutions; however, the UN is in a unique position to recognize where there is commonality and agreement across forums and institutions and to then codify that agreement. Such formal codification can help to enable more meaningful implementation.

- Leverage the Global Commitment on Digital Trust and Security. The UN Global Commitment on Digital Trust and Security represents an important effort that can help create continuity and cohesion across the ongoing dialogues at the UN, while also integrating the perspectives of the multistakeholder community. Early on, the Global Commitment can have a positive impact by bringing existing efforts and agreements together, leveraging diverse stakeholder inputs, and driving codification and implementation.

We would like to thank the Australian government once again for the opportunity to share our perspectives as they relate to these important dialogues. We hope these responses provide a helpful contribution in

Microsoft Corporation Tel 425 882 8080
One Microsoft Way Fax 425 936 7329
Redmond, WA 98052-6399 http://www.microsoft.com/

advancing a shared objective: achieving a rules-based and rights-respecting online world for all. More than anything else, we believe accomplishing this requires trust and cooperation across stakeholder groups with responsibilities in this space, underscoring the value of precisely this sort of outreach. Please let us know if we can provide any additional input or clarify any of the contributions provided here and we look forward to additional opportunities to collaborate in the future.