Microsoft response to the UN High-level Panel on Digital Cooperation report on the Age of Digital Interdependence

September 2019

Summary

The report developed by the United Nations (UN) Secretary-General's High-level Panel on Digital Cooperation, "The Age of Digital Interdependence," marks a decisive moment in time – one in which the future of technology and society will be impacted by critical decisions we make about our digital growth, interdependence, and cooperation. Microsoft appreciates the UN Secretary-General's initiative and the hard work of the High-level Panel in developing a comprehensive report and in gathering perspectives from a broad spectrum of stakeholders. We also welcome the recognition that multi-stakeholderism should be at the heart of efforts to enhance digital cooperation and that an increased role for multi-stakeholder cooperation is needed within the UN System. This is aligned with our vision of the private sector having both expertise and a responsibility to contribute to addressing the challenges arising from ongoing global digital transformation.

Empowering others to achieve more is our company's core mission. Strengthening digital access and inclusion, respecting human rights, and fostering digital trust and security are all foundational to that mission. As such, across each of the Panel's recommendations, we welcome the opportunity to provide input and to contribute to efforts to realize outcomes that help to advance digital cooperation. We also regard the UN's role in driving digital trust and security forward particularly important. In the face of increasing cyber threats, the implementation of international norms for responsible behavior in cyberspace is critical, and there is an opportunity in the near term to leverage the momentum of several ongoing processes to make meaningful progress. We are committed to working in earnest with the UN and with other key actors to do so, building out a clear and coherent vision for the future and driving action that will enable achievement of the outcomes that we collectively articulate.

Below, we provide feedback and ideas related to each of the Panel's recommendations, including both the issue areas and the detailed recommendations themselves. We also highlight examples of initiatives that are ongoing and that could be further leveraged or supported. We welcome the opportunity to engage further with the UN on each of these important areas and to continue to not only build a robust dialogue but also advance urgent action with all stakeholders on digital cooperation.

An Inclusive Digital Economy and Society

Policymakers must retain a primary focus on the foundational issue of connectivity – without it, the potential of digital transformation to equip populations, governments, and civil society with tools to achieve the 2030 Agenda for Sustainable Development will remain challenging.

> *High-level Panel Recommendation 1A - We recommend that by 2030, every adult should have affordable access to digital networks, as well as digitally-enabled financial and health services, as a means to make a substantial contribution to achieving the SDGs. Provision of these services should guard against abuse by building on emerging principles and best practices, one example of which is providing the ability to opt in and opt out, and by encouraging informed public discourse.*

We strongly agree with the Panel's recommended commitment to universal affordable access to the Internet by 2030. Microsoft supports affordable and universal access to broadband services and the

Internet, and we make a practical contribution to this goal through our Airband Initiative.[1] This global Initiative grew out of an initial desire to help provide Internet access to the estimated 19 million people living in rural communities of the United States without access to high-speed broadband connections, demonstrating that this is a policy challenge in both developed and developing economies. We therefore agree with the report's observation that "Internet access in many parts of the world is still too slow and expensive to be effectively used," and we not only support the aspiration of universal affordable Internet access by 2030 but also believe that it is vital to keep focus on this foundational issue. Without continued attention by policy-makers to expand access, the potential of digital transformation to equip populations with tools to relieve poverty, access education, and benefit from "digitally-enabled financial and health services" will remain a secondary issue.

In seeking to meet the goal set out in Recommendation 1A, governments and regulators should enact policies that can show measurable and meaningful progress. One necessary element will be to have a clear and ambitious definition of what counts as "affordable." In that regard, we commend the affordability target set out by the Alliance for Affordable Internet (A4AI) and already taken up by some countries. The A4AI proposes a "1 for 2" affordability target to be tailored to a given country or region – 1GB of mobile broadband priced at 2 percent or less of average monthly income.[2]

Another important aspect of designing appropriate and impactful policies is to maximize availability and accuracy of data on connectivity. In the United States, Microsoft has highlighted shortcomings in the Federal Communication Commission's broadband data, making invisible millions of Americans already lacking access to broadband and substantially decreasing the likelihood of additional broadband funding or much-needed broadband service.[3] We proposed improvements to broadband mapping in the United States to extend and enhance the collection of availability data, providing more accurate and more granular data and incorporating actual usage or subscription data, which ultimately enables a more well-rounded view. Reflecting on the availability and accuracy of data relating to broadband coverage is an important part of addressing the overall issue of affordable access, whether that be at the international level or with national governments and regulators.

> *High-level Panel Recommendation 1B - We recommend that a broad, multi-stakeholder alliance, involving the UN, create a platform for sharing digital public goods, engaging talent and pooling data sets, in a manner that respects privacy, in areas related to attaining the SDGs.*

Microsoft believes that it is important to enable the responsible sharing of data in ways that further innovation while not adversely impacting investments made by private actors. As a company, we are committed to helping individuals and organizations around the world leverage data to solve a wide range of societal and business problems. However, such data sharing can be extremely challenging today, in part because of a lack of standards that define how data sets can be used.

We think there is an opportunity to reduce the friction of data sharing by offering a set of legal, licensing, and governance tools for consideration by interested communities, and we have announced and released materials to support an initiative to encourage more responsible data sharing.[4] Specifically, we view our proposed Data Use Agreement templates as a starting point to explore and learn from the community about the types of scenarios where such agreements may be helpful. We

[1] https://www.microsoft.com/en-us/airband
[2] http://a4ai.org/wp-content/uploads/2016/09/Redefining-Affordability_1-for-2-Target.pdf
[3] https://blogs.microsoft.com/on-the-issues/2019/04/08/its-time-for-a-new-approach-for-mapping-broadband-data-to-better-serve-americans/
[4] https://news.microsoft.com/datainnovation/

intend to work with stakeholders in the community to understand needs in different sectors so we can collectively work towards a common framework that makes it easier to execute Data Use Agreements, establish a set of standard clauses for data sharing, and more. With these agreements, our hope is to contribute to the communities interested in facilitating more open and collaborative approaches to using data and to show our commitment to being more open with our data and efforts to develop Artificial Intelligence (AI), including in ways that support the attainment of the Sustainable Development Goals.

> *High-level Panel Recommendation 1C - We call on the private sector, civil society, national governments, multilateral banks and the UN to adopt specific policies to support full digital inclusion and digital equality for women and traditionally marginalised groups. International organisations such as the World Bank and the UN should strengthen research and promote action on barriers women and marginalised groups face to digital inclusion and digital equality.*

We strongly support Recommendation 1C. Beyond providing affordable access (as discussed under Recommendation 1A), Microsoft believes that local capacity building is important to enable not just adoption, but also production and consumption, of localized content and services. Such capacity building could include training for young people and disadvantaged populations, particularly girls, as well as support for local small- and medium-sized enterprises. For its part, Microsoft has created and made available a wide range of curriculum, content, and programs to support the needs of all learners across the digital skills spectrum — from foundational digital literacy to computer science education.[5] For example, we support Women in Cloud, a community-led initiative supporting female technology entrepreneurs, within which Microsoft's Cloud Accelerator Program helps women-led companies start and build their businesses.[6] In addition, technology provides many opportunities to protect or enable disadvantaged groups. With AI for Humanitarian Action, we leverage AI to support disaster recovery, address the needs of children, and protect displaced people.[7] Similarly, AI for Accessibility is a grant program that harnesses the power of AI to amplify human capability for the more than one billion people around the world with a disability.[8]

> *High-level Panel Recommendation 1D - We believe that a set of metrics for digital inclusiveness should be urgently agreed, measured worldwide and detailed with sex disaggregated data in the annual reports of institutions such as the UN, the International Monetary Fund, the World Bank, other multilateral development banks and the OECD. From this, strategies and plans of action could be developed.*

Microsoft agrees that it would be valuable to agree to a set of metrics for digital inclusiveness. Rather than creating a net new set of metrics, we suggest leveraging the ideas and metrics set out by the UN's Broadband Commission, which has done some measurement and reporting on gender equality. For example, Target 7[9] states that "by 2025 gender equality should be achieved across all targets" (other targets are measures of affordability, connectivity, skills, access, and other enabling policies). Of course, defining the metrics is only the starting point, and availability and accuracy of data will also be important topics to consider – given that the necessary data, e.g. disaggregated by gender, might not be widely available. In addition, there may be metrics from other contexts that provide valuable lessons,

[5] https://www.microsoft.com/en-us/philanthropies/empowering-people
[6] https://blogs.microsoft.com/blog/2019/06/05/microsoft-backs-women-tech-entrepreneurs-with-global-expansion-of-ideagen-and-women-in-cloud/
[7] https://www.microsoft.com/en-us/ai/ai-for-humanitarian-action
[8] https://www.microsoft.com/en-us/ai/ai-for-accessibility
[9] https://www.broadbandcommission.org/Pages/targets/Target-7.aspx

such as the Access to Medicine Index. The Access to Medicine Index may suggest how the information and communications technology industries can be measured in terms of ensuring that technology is available, affordable, accessible, and acceptable in low- and middle-income countries.[10]

Human and Institutional Capacity

Microsoft believes that investing in capacity building is an important element of improving global digital cooperation and attaining the Sustainable Development Goals. This can best be accomplished by strengthening existing systems and processes that are largely working to address gaps rather than by creating wholly new and potentially duplicative systems. Microsoft currently invests in a range of initiatives to promote greater understanding of digital technologies and to help inform policymaker decisions. For instance, we are directly engaged in the Global Forum on Cyber Expertise,[11] the United Kingdom's Foreign & Commonwealth Office Cyber Security Capacity Building Programme,[12] and the United States Telecommunications Training Institute.[13] Through the Cybersecurity Tech Accord, we are also contributing to efforts to share materials on a range of topics, such as cloud computing.[14] We are also a founding member and co-chair of the Cyber Readiness Institute, which is focused on promoting cyber risk management efforts with SMBs around the world.[15]

> *High-level Panel Recommendation 2 - We recommend the establishment of regional and global digital help desks to help governments, civil society and the private sector to understand digital issues and develop capacity to steer cooperation related to social and economic impacts of digital technologies.*

We believe that providing a resource to help various stakeholders understand what resources exist and how to improve their understanding of a range of topics would help to amplify the impact of existing capacity building efforts. It may also help those investing in capacity building better understand demand signals and where additional investments might be most impactful. We further elaborate on this recommendation below (under the header of Global Digital Cooperation: Recommendation 5) in considering the various proposals for and elements of digital cooperation architectures, including the "Observatory and Help Desk" element of the IGF Plus proposal.

Human Rights and Human Agency

We are encouraged by the Panel's focus on the protection of human rights in the digital world. We fully agree that human rights apply online as well as offline and are central to discussions around the digital economy. Further, we believe that acknowledging the two-way dynamic between technology and human rights is important: technology should respect human rights (as the report highlights), and technology can also empower the exercise of human rights. Ultimately, technology that most effectively respects human rights also most effectively empowers the exercise of human rights.

The report includes important high-level principles that help to elucidate a desirable future, and we think a valuable next step would involve identifying the policies and processes needed to bring those principles to life. We also encourage future UN efforts to focus on helping to drive broad, inclusive, and multidisciplinary thinking on the harder AI governance challenges.

---

[10] https://accesstomedicinefoundation.org/access-to-medicine-index
[11] https://www.thegfce.com/
[12] https://www.gov.uk/government/publications/fco-cyber-security-capacity-building-programme-2018-to-2021
[13] http://ustti.org/
[14] https://cybertechaccord.org/webinars/
[15] https://www.cyberreadinessinstitute.org/

High-Level Panel Recommendation 3A - Given that human rights apply fully in the digital world, we urge the UN Secretary-General to institute an agencies-wide review of how existing international human rights accords and standards apply to new and emerging digital technologies. Civil society, governments, the private sector and the public should be invited to submit their views on how to apply existing human rights instruments in the digital age in a proactive and transparent process.

Codifying how human rights standards apply to digital technologies is essential, and Microsoft welcomes the opportunity to contribute to efforts to do so in partnership with the UN Office of the High Commissioner on Human Rights and other stakeholders. As a starting point, leveraging learnings from efforts that resulted in the Convention on the Rights of Persons with Disabilities[16] and that created the Free and Equal campaign,[17] the UN and partner organizations could create a catalogue or compendium that sets out the legal obligations that States have towards human rights online, contributing to debate at not only the global level but also the national level, which is where implementation needs to occur.[18] This sort of document could help to authoritatively identify how the international regime covers the full spectrum of rights as well as whether and where there may be gaps that need to be filled through new international agreements. A compendium could also help governments identify how they can ensure alignment between legislation and international norms, help companies understand requirements that are applicable to their operations, empower civil society to drive change at the national level, and inform the Human Rights Council on these critical issues.

High-level Panel Recommendation 3B - In the face of growing threats to human rights and safety, including those of children, we call on social media enterprises to work with governments, international and local civil society organisations and human rights experts around the world to fully understand and respond to concerns about existing or potential human rights violations.

Microsoft has a responsibility to manage our services so that they are tools of empowerment for people to exercise their rights online through a safe and inclusive Internet. We also have a responsibility to manage our services in a way that respects universal human values, like privacy and freedom of expression.

[16] https://www.un.org/development/desa/disabilities/convention-on-the-rights-of-persons-with-disabilities.html
[17] https://www.unfe.org/
[18] For example, using language from the compendium for the Free and Equal campaign, it is possible to outline one option for what this might look like: "The purpose of this compendium is to set out the core obligations that States have towards human rights in connection to technologies (including but not limited to the Internet, the Internet of Things, robotics, and more), and describe how the United Nations mechanisms have applied international law in this context. For many years, UN human rights treaty bodies and special procedures have documented violations of the human rights of people as a result of new and emerging technologies and analyzed State compliance with international human rights law. They have accumulated a body of evidence that shows how individuals are impacted on the basis of their online activities and connected devices and have issued specific guidance to States. The sections of the compendium should summarize their findings and advice to help States take the necessary steps to meet their fundamental human rights obligations. The compendium is also intended to assist human rights defenders and rights-holders generally to call States to account for breaches of international human rights law. // The compendium consists of "X" sections. Each section sets forth a State obligation, the relevant international human rights law, and the views of human rights treaty bodies and special procedures. Excerpts from their reporting give examples of the kinds of abuses experienced and paint a broad picture of widespread challenges. Each section concludes with recommendations to States. // The protection of people on the basis of their internet and technology use does not require the creation of new rights or special rights. Rather, it requires enforcement of the universally applicable guarantee of the enjoyment of all rights in every aspect of life."

We recognize that this is an area where no single company, body or stakeholder will have all the answers. This is the type of serious challenge that requires broad discussion and collaboration with people in governments and across civil society, and it needs companies across the tech sector to learn, think, work, and act together. As a founding member of the Global Internet Forum to Counter Terrorism (GIFCT), Microsoft works with other major technology companies that have collectively gained considerable experience in tackling extremist and violent content on our platforms. In addition, in May 2019, Amazon, Facebook, Google, Twitter and Microsoft jointly not only announced their support for the Christchurch Call to Action To Eliminate Terrorist and Violent Extremist Content Online but also published nine steps that each company will take to implement the Christchurch Call.[19]

Microsoft is also committed to creating a safer online environment for youths and adults through education, development of new technology tools and techniques, and collaboration with international organizations and other stakeholders. Through research and advocacy in more than 20 countries, for the past four years, Microsoft has been promoting "digital civility"[20] in all online interactions by encouraging people to lead and act with empathy, compassion, and kindness.

> *High-Level Panel Recommendation 3C - We believe that autonomous intelligent systems should be designed in ways that enable their decisions to be explained and humans to be accountable for their use. Audits and certification schemes should monitor compliance of artificial intelligence (AI) systems with engineering and ethical standards, which should be developed using multi-stakeholder and multilateral approaches. Life and death decisions should not be delegated to machines. We call for enhanced digital cooperation with multiple stakeholders to think through the design and application of these standards and principles such as transparency and non-bias in autonomous intelligent systems in different social settings.*

Microsoft believes that AI offers incredible opportunities to drive widespread economic and social progress and can help to realize the Sustainable Development Goals. We are already seeing the application of a variety of tools that will generate the insights on which we can build healthier, cleaner, more prosperous societies.[21] Examples range from protecting biodiversity[22] and tracking endangered species[23] to transforming agriculture[24] and improving healthcare.[25] However, in an era in which digital technology is changing almost every aspect of how people live, work, play, and learn, we understand and believe that it is important to think carefully about the complex questions that AI raises.

Designing AI to be trustworthy requires creating solutions that reflect principles that are deeply rooted in important and universal rights. At Microsoft, we've identified six principles – fairness, reliability and safety, privacy and security, inclusivity, transparency, and accountability – to guide the cross-disciplinary development and use of artificial intelligence.[26] In the context of facial recognition technology in particular, we've also adopted six overlapping and complementary principles – fairness,

---

[19] https://blogs.microsoft.com/on-the-issues/2019/05/15/the-christchurch-call-and-steps-to-tackle-terrorist-and-violent-extremist-content/
[20] https://www.microsoft.com/en-us/digital-skills/digital-civility
[21] https://www.microsoft.com/en-us/ai/ai-for-good
[22] https://news.microsoft.com/europe/2019/08/13/protecting-biodiversity-with-shazam4nature/
[23] https://news.microsoft.com/on-the-issues/2019/08/06/ai-endangered-species/
[24] https://blogs.microsoft.com/blog/2019/08/07/harnessing-the-power-of-ai-to-transform-agriculture/
[25] https://blogs.microsoft.com/ai/microsoft-healthcare-bot-service/
[26] https://blogs.microsoft.com/wp-content/uploads/2018/02/The-Future-Computed_2.8.18.pdf (see pgs. 57-73 for a discussion of the principles of fairness, reliability and safety, privacy and security, inclusivity, transparency, and accountability)

transparency, accountability, non-discrimination, notice and consent, and lawful surveillance – that address concerns related to that particular application of AI technology.[27]

We also commend the Organization for Economic Co-operation and Development (OECD) Principles on Artificial Intelligence,[28] which have been adopted by 42 countries and by the G20. The signatories to these intergovernmental policy guidelines on AI have agreed to uphold international standards that aim to ensure AI systems are designed to be robust, safe, fair, and trustworthy. In addition, the OECD has created an AI Policy Observatory[29] that will combine resources from across the OECD with those of partners from all stakeholder groups to provide multidisciplinary, evidence-based policy analysis on AI and to facilitate dialogue.

We agree that there would be value in convening multi-stakeholder discussion about the design and application of principles such as transparency, explainability, and accountability in different applications and settings. However, we caution the UN regarding the Panel's recommendation with regard to audits and certification schemes; while we agree that such mechanisms should be developed through multi-stakeholder forums and will be helpful for understanding and monitoring compliance, we also note that, at this developmental stage of the technology, locking in such mechanisms may be premature. Rather, discussions should be about guiding the responsible development of AI to be human-centered and, in our view, the focus should be in two areas. Firstly, it is important to share and discuss best practices in the way AI is being applied in different sectors. Secondly, we need broad and inclusive thinking on the harder AI governance challenges and on how companies can operate with sufficient accountability to foster confidence in the benefits that we are striving to make possible. Further, given its leadership on AI principles, we recommend engaging in activities coordinated by the OECD. For specific applications, there may also be other appropriate conveners, such as the UN Office for Disarmament Affairs.

Realizing the potential of AI will require all stakeholders to share responsibility in shaping its development to be trustworthy, including by enabling explainability and accountability. Technologists will need to work closely with governments, academia, industry, civil society, and other stakeholders. Moreover, AI is a great example of the importance of multidisciplinary policymaking; skilling-up for an AI-powered world involves more than science, technology, engineering, and math. As computers ascertain capabilities that are comparable to human skills, learnings from the social sciences and humanities will become even more important to incorporate. Languages, art, history, economics, ethics, philosophy, psychology, and human development courses can teach critical philosophical and ethics-based skills that will be instrumental in the development and management of AI solutions.

Trust, Security and Stability

Technology has become intertwined with nearly all aspects of daily life, and the protection of civilians and civilian infrastructure requires that we recognize the importance of digital security and take action to mitigate the risks that may undermine our digital stability if unaddressed. We are encouraged by the Panel's focus on digital trust, security, and stability and its acknowledgement of a range of security issues as well as its focus on efforts to coalesce and strengthen the development and implementation of international norms for responsible behavior in cyberspace. This is an area of critical importance and one in which the UN is a key driver of the alignment and action needed to realize a more stable, secure, and trusted cyberspace. Moreover, for such efforts, the Panel's recognition of the importance of going beyond multilateral discussions and leveraging the expertise and commitments of all relevant stakeholders – i.e., through a multi-stakeholder approach – is especially valuable; unprecedented

[27] https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/
[28] https://www.oecd.org/science/forty-two-countries-adopt-new-oecd-principles-on-artificial-intelligence.htm
[29] https://www.oecd.org/going-digital/ai/about-the-oecd-ai-policy-observatory.pdf

agreements will require unprecedented coordination, including through processes that are transparent and managed by institutions that are focused on building consensus and progressing toward meaningful outcomes.

> *High-level Panel Recommendation 4 - We recommend the development of a Global Commitment on Digital Trust and Security to shape a shared vision, identify attributes of digital stability, elucidate and strengthen the implementation of norms for responsible uses of technology, and propose priorities for action.*

We strongly agree with the Panel's recommendation of developing a Global Commitment on Digital Trust and Security, and we're keen to contribute to efforts to shape and realize a shared vision of digital stability. In providing context for its call for a multi-stakeholder Global Commitment on Digital Trust and Security, the Panel recognizes that many past and currently ongoing initiatives[30] on digital trust, security, and stability have made important progress and that a Global Commitment could bolster and coordinate across these efforts with a focus on supporting implementation of agreed norms, rules, and principles of responsible behavior. We believe that there would be tremendous value in demonstrating agreement and continuity across initiatives and in focusing on implementation. While ongoing initiatives – such as the Paris Call for Trust and Security in Cyberspace (Paris Call) – can continue to utilize their unique compositions and agile processes to facilitate progress, there is also a need for the UN to leverage its unparalleled convening power and voice to help bring to the fore where agreement exists and where and how implementation should proceed in earnest.

To demonstrate the important point that the Panel raised about the value of a Global Commitment bolstering and coordinating across past and ongoing efforts, a table in Appendix A highlights some of the areas in which overlap or agreement has emerged (in initiatives highlighted by the Panel explicitly as well as others). This is not intended to be a comprehensive evaluation of relevant efforts and existing overlap but rather an example of work the Global Commitment could further pursue and endorse as well as leverage to determine appropriate next steps for implementation or other action.

We would welcome the opportunity to further contribute to such efforts or to think both imaginatively and practically with committed stakeholders about other ways that the Global Commitment could facilitate greater cohesion across past and ongoing initiatives and accelerate progress toward trust, security, and stability. We encourage the UN to identify organizations that represent various stakeholder groups and that can work cooperatively to scope an agenda for the Global Commitment – and then take action to broaden consensus and drive toward meaningful outcomes.

The Global Commitment must carry forward the consensus that exists today, bringing creative energy and partnership to the challenge of realizing agreed-upon commitments, including through attention to implementation and accountability. To do so, it may consider innovative models for collaborating in an ongoing way with partners in the private sector and civil society communities, further leveraging the benefit a multi-stakeholder approach brings to this space – as demonstrated by the Paris Call. The Global Commitment should also coordinate with, complement, and seek to leverage the learnings of the current GGE and OEWG processes, which could further demonstrate continuity and cohesion of important efforts in this space as well as where next steps might be warranted. It could also help to facilitate further multi-stakeholder engagement in both the GGE and OWEG processes.

[30] For instance, the Panel's report references the UN Groups of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, the Paris Call for Trust and Security in Cyberspace, the Global Commission on Stability in Cyberspace, the Global Conference on Cyberspace (i.e., "London Process"), the Geneva Dialogue on Responsible Behavior in Cyberspace, the Cybersecurity Tech Accord, and the Charter of Trust. It also references the two newest processes, the 2019 UN GGE and Open-Ended Working Group (OEWG).

With regard to the Panel's proposal that the Global Commitment on Digital Trust and Security could identify attributes of digital stability, we propose the following attributes for consideration: open, cooperative environment that has operationalized multi-stakeholder engagement; trust in technology to function as expected; resilient connection and interconnection, including through the protection of civilians and civilian infrastructure, such as electoral processes; free flow of information consistent with appropriate laws; and trust in institutions to hold malicious actors accountable. Notably, norms to codify responsible use of technology – as well as mechanisms, potentially including more robust, multi-stakeholder institutional structures, to strengthen the implementation of those norms – are critical enablers of efforts to hold actors accountable.

Global Digital Cooperation

We agree that improved cooperation is needed and considered with interest the Panel's ideas and recommendations around digital cooperation architectures. IGF Plus has the notable advantage of building on an existing mechanism that can be improved more quickly, and we can draw on learnings from the IGF to inform what needs to change and how. We support efforts to evolve the IGF through exploring and implementing the various IGF Plus mechanisms outlined in the report and by linking the IGF Plus Secretariat to the Office of the United Nations Secretary-General. We also note that these important efforts will be most successful with a stable and appropriate budget allocated for IGF Plus.

> *High-level Panel Recommendation 5A - We recommend that, as a matter of urgency, the UN Secretary-General facilitate an agile and open consultation process to develop updated mechanisms for global digital cooperation, with the options discussed in Chapter 4 as a starting point. We suggest an initial goal of marking the UN's 75th anniversary in 2020 with a "Global Commitment for Digital Cooperation" to enshrine shared values, principles, understandings and objectives for an improved global digital cooperation architecture. As part of this process, we understand that the UN Secretary-General may appoint a Technology Envoy.*

We appreciate the opportunity to further deliberate on and contribute ideas regarding mechanisms for global digital cooperation. Of the three digital cooperation architectures proposed, we see the most promise in the IGF Plus model. A clear advantage is that the model builds on something that already exists. As such, it is a platform that stakeholders and policymakers are familiar with, and building on an existing model means there is no need to start from scratch or invent something new and potentially duplicative. Moreover, there are plenty of learnings that can inform what needs to change and how.

We also believe that, although the Panel highlighted "lack of actionable outcomes" as a shortcoming of the current IGF, the forum does enable achievement of meaningful and actionable outcomes. The unique value of the IGF lies in its nature as a multi-stakeholder forum for discussion and exchange of views, open to all, without the pressure of necessarily having to negotiate written declarations. The importance of the IGF physically bringing together people from different backgrounds, perspectives and parts of the world, and the new connections and viewpoints that are then formed, should not be underestimated. As such, we believe that transforming the IGF, such as by expecting it to produce more formal or binding written outputs that would turn the IGF into a negotiating forum, might frustrate the energy that enables such a rich exchange of – as well as development or evolution of – views. Indeed, retaining significant space within an IGF Plus to continue serving as a forum where views are exchanged and people can learn from each other will be important for tackling what the report describes as a "lack of trust among governments, civil society and the private sector – and sometimes a lack of humility and understanding of different perspectives."

There also already exist a number of written outputs, ranging from the reports of the IGF's Best Practices Forums and Dynamic Coalitions to the summaries of the various sessions held at each IGF meeting. The wealth of ideas and information collected over the years provides a sound basis for a Help Desk function within an IGF Plus – the challenge is to find ways to ensure that the existing written outputs are better organized and marketed, something that the under-resourced IGF Secretariat has not been able to consistently do.

Microsoft has been directly involved in two concrete outcomes that suggest there is an opportunity to leverage and strengthen the IGF towards creation of more actionable outputs that are well supported by the multi-stakeholder community:

- An early demo of Microsoft's TV White Spaces technology at the 2011 IGF meeting in Nairobi was key to the development of our Airband Initiative,[31] which partners with organizations to utilize TV Whites Space (TVWS) devices and other low-cost wireless technologies to make it easier and more affordable for people to get online. The Airband Initiative was launched in July 2017 and is committed to bringing broadband access to 3 million Americans in rural areas by July 2022. In addition, the Initiative is now responsible for putting in place commercial deployments and pilots connecting the unconnected in over 30 countries around the world.

- The text of the Paris Call for Trust and Security in Cyberspace[32] was developed by experts outside of the IGF, but President Macron chose to formally launch it at the 2018 IGF meeting alongside the inaugural Paris Peace Forum. By bringing attention to the Paris Call at the IGF, its messages and call for action were amplified, widening the engaged audience and adding momentum to efforts to broaden support. The IGF therefore provided a platform for amplification, exposing the issues to a key group of stakeholders.

Our direct experience bodes well for the Report's recommendations for an IGF Plus to take on the roles of Policy Incubator and Cooperation Accelerator.

As a next step, we propose that the IGF Secretariat should conduct a survey to collect examples and experiences to better understand what outcomes have already been achieved through and better understand how the IGF already contributes to digital cooperation. These could provide useful input to those who take responsibility for developing the functions envisaged for an IGF Plus.

In addition, in our experience, one of the reasons why the impact of the IGF may be constrained is the lack of formal recognition by the UN system in the form of direct funding to supports its activities. The limited and unstable budget afforded by voluntary donations to the IGF Trust Fund has significantly limited what the IGF has been able to do, e.g. in terms of its reach, its momentum, and its ability to leverage the insights gained via the interactions in the meetings and in producing its written outputs. The lack of direct funding from the UN budget also means that the hosting of the event has to be paid for entirely by the host government, limiting the distribution of countries able to host the event. Specifically, direct funding from the UN budget or other innovative sources could therefore enable a wider and more diverse pool of governments to offer to host the event.

In summary, we support efforts to evolve the IGF through exploring and implementing the various IGF Plus mechanisms outlined in the report and by linking the IGF Plus Secretariat to the Office of the

[31] https://www.microsoft.com/en-us/airband
[32] https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in

United Nations Secretary-General. However, we are concerned that its success will be limited without the UN recognizing the valuable role of such an expanded IGF by funding it appropriately.

> *High-level Panel Recommendation 5B - We support a multi-stakeholder "systems" approach for cooperation and regulation that is adaptive, agile, inclusive and fit for purpose for the fast-changing digital age.*

We agree with the various elements of this recommendation. We see a central role for soft governance mechanisms, such as values and principles, and we support the vision of a "a fact-based, participative process of deliberation and design, including governments, private sector, civil society, diverse users and policy-makers." To that point, we warmly welcome the Panel's articulation of nine values that shape digital cooperation – inclusiveness, respect, human-centredness, human flourishing, transparency, collaboration, accessibility, sustainability, harmony. We believe that these nine values, described in detail on page 7 of the report, should be at the heart of any Global Commitment for Digital Cooperation that is produced. We also welcome a holistic "systems" approach of bringing together appropriate government agencies, regulators, and stakeholders to be able to respond to issues with agility.

Appendix A: Table Comparing Norms Across Processes

As highlighted above in the text, note that this table is not intended to be a comprehensive evaluation but rather an example of some of the global forums, processes, and issues wherein overlap or agreement has emerged and of work that the Global Commitment on Digital Trust and Security could further pursue and endorse as well as leverage to determine appropriate next steps for implementation or other action. It is comprehensive neither in terms of norms or "issues" referenced nor in terms of "processes" (e.g., Paris Call for Trust & Security in Cyberspace) included. The processes and sources included are intended to be a sample of a range of global efforts on cyber norms.

Further, norms referenced by different processes in the context of a particular issue (e.g., protecting the public and critical infrastructure) are not necessarily identical; in some cases, the overlap is limited to common attention to an issue, and significantly different behavioral expectations or values may be emphasized. In other cases, the overlap may be more extensive, but there may still be different points of emphasis. The overall goal is to demonstrate that there are substantial commonalities in areas that States and other actors have focused on in the context of global cybersecurity and norm building.

Finally, note that the table is organized by frequency of references; the more the processes included address the highlighted issue, the earlier in the table it appears.

Comparing Cyber Norms Across Processes					
Issue	**UN Group of Governmental Experts (GGE) Consensus Report (2015)**	**Shanghai Cooperation Organization (SCO) Code of Conduct (Revised, 2015)**	**Paris Call for Trust & Security in Cyberspace (2018)**	**Global Commission on Cyber Stability (2019)**	**Other Sources**
Protecting the Public and Critical Infrastructure	**¶13(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" **¶13(g):** "States should take appropriate measures to protect their critical infrastructure from ICT threats, taking	**¶2(6):** Participating States pledge "[t]o reaffirm the rights and responsibilities of all States, in accordance with the relevant norms and rules, regarding legal protection of their information space and critical information infrastructure against damage resulting from threats, interference, attack and sabotage"	**Principle 1:** Signatories affirm willingness to work together to "[p]revent and recover from malicious cyber activities that threaten or cause significant, indiscriminate or systemic harm to individuals and critical infrastructure"	**Norm 4:** "State and non-state actors should not commandeer the general public's ICT resources for use as botnets or for similar purposes."	OSCE Confidence Building Measures (2016), **No 15**: "Participating States, on a voluntary basis, will encourage, facilitate and/or participate in regional and subregional collaboration between legally-authorized authorities responsible for securing critical infrastructures to discuss opportunities and address challenges to national as well as trans-border ICT networks, upon which such critical infrastructure relies. Collaboration may, *inter alia*, include: – Sharing information on ICT threats; – Exchanging best practices; - Developing, where appropriate, shared responses to common challenges …" African Union Convention on Cyber Security and Personal Data Protection (not yet in force) **Art. 25(4)**: "Protection of critical infrastructure – Each State Party shall adopt such legislative and/or regulatory measures as they deem necessary to identify the sectors

Comparing Cyber Norms Across Processes					
Issue	**UN Group of Governmental Experts (GGE) Consensus Report (2015)**	**Shanghai Cooperation Organization (SCO) Code of Conduct (Revised, 2015)**	**Paris Call for Trust & Security in Cyberspace (2018)**	**Global Commission on Cyber Stability (2019)**	**Other Sources**
	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"				regarded as sensitive for their national security and well-being of the economy, as well as the information and communication technologies systems designed to function in these sectors as elements of critical information infrastructure …" G7 Taormina Leaders' Communiqué (2017) **¶15**: "... We will work together and with other partners to tackle cyber attacks and mitigate their impact on our critical infrastructures and the well-being of our societies." Cybersecurity Tech Accord (2018) **principle 2**: "WE WILL OPPOSE CYBERATTACKS ON INNOCENT CITIZENS AND ENTERPRISES FROM ANYWHERE. We will protect against tampering with and exploitation of technology products and services during their development, design, distribution and use. We will not help governments launch cyberattacks against innocent citizens and enterprises from anywhere."
Non-Interference in Internal Affairs (including electoral interference)	**¶28(b):** "In their use of ICTs, States must observe, among other principles of international law, State sovereignty, sovereign equality, the settlement of disputes by peaceful means and non-intervention in the internal affairs of other States."	**¶2(3):** "Participating States pledge "[n]ot to use information and communications technologies and information and communications networks to interfere in the internal affairs of other States or with the aim of undermining their political, economic and social stability."	**Principle 3**: Signatories affirm willingness to work together to "[s]trengthen our capacity to prevent malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities."	**Norm 2**: "State and non-state actors should not pursue, support or allow cyber operations intended to disrupt the technical infrastructure essential to elections, referenda or plebiscites."	Arab Convention on Combating Information Technology Offences, Art 4: "Safeguarding Sovereignty—1. Every State Party shall commit itself, subject to its own statutes or constitutional principles, to the discharge of its obligations stemming from the application of this convention in a manner consistent with the two principles of equality of the regional sovereignty of States and the non interference in the internal affairs of other States." G7 Charlevoix Commitment (2018): "We, the Leaders of the G7, commit to: Respond to foreign threats, both together and individually, in order to meet the challenges facing our democracies, Strengthen G7 cooperation to prevent, thwart and respond to malign interference by foreign actors aimed at

Comparing Cyber Norms Across Processes					
Issue	**UN Group of Governmental Experts (GGE) Consensus Report (2015)**	**Shanghai Cooperation Organization (SCO) Code of Conduct (Revised, 2015)**	**Paris Call for Trust & Security in Cyberspace (2018)**	**Global Commission on Cyber Stability (2019)**	**Other Sources**
					undermining the democratic processes and the national interests of a G7 state."
Ensuring Supply Chain Integrity	**¶13(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"		**Principle 6**: Signatories affirm willingness to work together to "[s]trengthen the security of digital processes, products and services, throughout their lifecycle and supply chain."	**Norm 3:** "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."	Cybersecurity Tech Accord (2018) **principles 1 and 3**: "We will design, develop, and deliver products and services that prioritize security, privacy, integrity and reliability, and in turn reduce the likelihood, frequency, exploitability, and severity of vulnerabilities. . . We will support civil society, governments and international organizations in their efforts to advance security in cyberspace and to build cybersecurity capacity in developed and emerging economies alike."
Protecting the Public Core of the Internet & its Governance		**¶2(8):** "All States must play the same role in, and carry equal responsibility for, international governance of the Internet, its security, continuity and stability of operation, and its development in a way which promotes the establishment of multilateral, transparent and democratic international Internet governance mechanisms which ensure an equitable distribution of resources, facilitate access for all and ensure the stable and secure functioning of the Internet"	**Principle 2**: Signatories affirm willingness to work together to "[p]revent activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet."	**Norm 1**: "NON-INTERFERENCE WITH THE PUBLIC CORE – Without prejudice to their rights and obligations, 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." (Defining "public core" "to include packet routing and forwarding, naming and	European Parliament Resolution (2018/2004(INI)) (2018), **clause 48**: "[E]ndorses the proposal that 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 cyber space;" NETmundial Multistakeholder Statement (2014): "Internet governance should be built on democratic, multistakeholder processes, ensuring the meaningful and accountable participation of all stakeholders, including governments, the private sector, civil society, the technical community, the academic community and users. The respective roles and responsibilities of stakeholders should be interpreted in a flexible manner with reference to the issue under discussion…"

Comparing Cyber Norms Across Processes					
Issue	**UN Group of Governmental Experts (GGE) Consensus Report (2015)**	**Shanghai Cooperation Organization (SCO) Code of Conduct (Revised, 2015)**	**Paris Call for Trust & Security in Cyberspace (2018)**	**Global Commission on Cyber Stability (2019)**	**Other Sources**
				numbering systems, the cryptographic mechanisms of security and identity, and physical transmission media.")	
Disclosing and Redressing Vulnerabilities	**¶13(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"	**¶2(5):** Participating States pledge "To endeavour to ensure the supply chain security of information and communications technology goods and services, in order to prevent other States from exploiting their dominant position in information and communications technologies, including dominance in resources, critical infrastructures, core technologies, information and communications technology goods and services and information and communications networks to undermine States' right to independent control of information and communications technology goods and services, or to threaten their political, economic and social security"		**Norm 5**: "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." **Norm 6:** "Developers and producers of products and services on which the stability of cyberspace depends should (1) prioritize security and stability, (2) take reasonable steps to ensure that their products or services are free from significant vulnerabilities, and (3) take measures to	OSCE Confidence Building Measures (2016), **No 16**: "Participating States will, on a voluntary basis, encourage responsible reporting of vulnerabilities affecting the security of and in the use of ICTs and share associated information on available remedies to such vulnerabilities, including with relevant segments of the ICT business and industry, with the goal of increasing co-operation and transparency within the OSCE region." Cybersecurity Tech Accord (2018) **principle 4**: "WE WILL PARTNER WITH EACH OTHER AND WITH LIKEMINDED GROUPS TO ENHANCE CYBERSECURITY. We will work with each other and will establish formal and informal partnerships with industry, civil society, and security researchers, across proprietary and open source technologies to improve technical collaboration, coordinated vulnerability disclosure, and threat sharing, as well as to minimize the levels of malicious code being introduced into cyberspace." Global Forum on Cyber Expertise, Coordinated Vulnerability Disclosure Manifesto: "Signatories to the Coordinated Vulnerability Disclosure [Manifesto] commit to implement public reporting mechanisms on vulnerabilities in their ICT systems and call upon other organizations to do the same. The Manifesto aims to make all parties more aware of the importance

Comparing Cyber Norms Across Processes					
Issue	**UN Group of Governmental Experts (GGE) Consensus Report (2015)**	**Shanghai Cooperation Organization (SCO) Code of Conduct (Revised, 2015)**	**Paris Call for Trust & Security in Cyberspace (2018)**	**Global Commission on Cyber Stability (2019)**	**Other Sources**
				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."	of cooperation to improve cybersecurity for everyone."
Applying International Law	**¶25**: "The adherence by States to international law, in particular their Charter obligations, is an essential framework for their actions in their use of ICTs and to promote an open, secure, stable, accessible and peaceful ICT environment…" **¶26**: "In considering the application of international law to State use of ICTs, the Group identified as of central importance the commitments of States to the following principles of the Charter and other international law: sovereign equality; the settlement of international disputes by peaceful	**¶2(1):** Participating States pledge "[t]o comply with the Charter of the United Nations and universally recognized norms governing international relations that enshrine, inter alia, respect for the sovereignty, territorial integrity and political independence of all States, respect for human rights and fundamental freedoms and respect for the diversity of history, culture and social systems of all countries." **¶2(12):** Participating States pledge "[t]o . . . promote a prominent role for the United Nations			UN General Assembly Resolution 70/237 (2015): "Welcoming the conclusion of the Group of Governmental Experts in its 2013 report that international law, and in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful information and communications technology environment …" G7 Declaration on Responsible States Behavior in Cyberspace (2017): "We reaffirm and note with approval the widespread affirmation by other States that international law and, in particular, the United Nations Charter is applicable to the use of ICTs by States. This affirmation is essential to maintaining peace and security and promoting an open, secure, stable, accessible and peaceful ICT environment;" G20 Antalya Summit Leader's Communique (2015) **¶26**: "We also note the key role played by the United Nations in developing norms and in this context we welcome the 2015 report of the UN Group of Governmental Experts in the Field of Information and Telecommunications in the Context of

Comparing Cyber Norms Across Processes					
Issue	**UN Group of Governmental Experts (GGE) Consensus Report (2015)**	**Shanghai Cooperation Organization (SCO) Code of Conduct (Revised, 2015)**	**Paris Call for Trust & Security in Cyberspace (2018)**	**Global Commission on Cyber Stability (2019)**	**Other Sources**
	means in such a manner that international peace and security and justice are not endangered; refraining in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the United Nations; respect for human rights and fundamental freedoms; and non-intervention in the internal affairs of other States." **¶27**: "State sovereignty and international norms and principles that flow from sovereignty apply to the conduct by States of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory."	in areas such as encouraging the development of international legal norms for information security."			International Security, affirm that international law, and in particular the UN Charter, is applicable to state conduct in the use of ICTs and commit ourselves to the view that all states should abide by norms of responsible state behaviour in the use of ICTs in accordance with UN resolution A/C.1/70/L.45;" European Parliament Resolution (2018/2004(INI)) (2018) **cl. 48**: Parliament "[c]onfirms its full commitment to an open, free, stable and secure cyber space . . . where international disputes are settled by peaceful means on the basis of the UN Charter and principles of international law;" Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2017) Introduction (p. 3): "Both International Groups of Experts were unanimous in their estimation that international law applies to cyber operations, an assessment now shared by most States and acknowledged by, *inter alia*, NATO and two United Nations Groups of Governmental Experts on Information Security in 2013 and 2015…"
Respecting Human Rights Online	**¶13(e):** "States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion,	**¶2(7):** Participating States pledge "[t]o recognize that the rights of an individual in the offline environment must also be protected in the			UN General Assembly Resolution 68/167 (2014) **operative cl. 3**: "Affirms that the same rights that people have offline must also be protected online, including the right to privacy;" UN HRC Resolution 34/7 (2017) **operative cl. 4**: "Affirms that the same

Comparing Cyber Norms Across Processes					
Issue	**UN Group of Governmental Experts (GGE) Consensus Report (2015)**	**Shanghai Cooperation Organization (SCO) Code of Conduct (Revised, 2015)**	**Paris Call for Trust & Security in Cyberspace (2018)**	**Global Commission on Cyber Stability (2019)**	**Other Sources**
	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" **¶28(b):** "States must comply with their obligations under international law to respect and protect human rights and fundamental freedoms"	online environment; to fully respect rights and freedoms in the information space, including the right and freedom to seek, receive and impart information, taking into account the fact that the International Covenant on Civil and Political Rights (article 19) attaches to that right special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a)for respect of the rights or reputations of others; (b)for the protection of national security or of public order (ordre public), or of public health or morals."			rights that people have offline must also be protected online, including the right to privacy;" UN Human Rights Council Resolution 32/13 (2016) **operative cl. 1**: "Affirms that the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with article 19 of the Universal Declaration of Human Rights and of the International Covenant on Civil and Political Rights;" G7 Declaration on Responsible States Behavior in Cyberspace (2017): "We also reaffirm that the same rights that people have offline must also be protected online and reaffirm the applicability of international human rights law in cyberspace, including the UN Charter, customary international law and relevant treaties;" The African Union Convention on Cyber Security and Personal Data Protection Art. 25(3) (not in force): "In adopting legal measures in the area of cyber security and establishing the framework for implementation thereof, each State Party shall ensure that the measures so adopted will not infringe on the rights of citizens guaranteed under the national constitution and internal laws and protected by international conventions, particularly the African Charter on Human and People's Rights and other basic rights such as freedom of expression …" Freedom Online Coalition Joint Statement on Internet Censorship (2018): "The FOC calls on all governments to refrain from content restrictions on the Internet that violate international human rights law and to create an enabling environment for free

Comparing Cyber Norms Across Processes					
Issue	**UN Group of Governmental Experts (GGE) Consensus Report (2015)**	**Shanghai Cooperation Organization (SCO) Code of Conduct (Revised, 2015)**	**Paris Call for Trust & Security in Cyberspace (2018)**	**Global Commission on Cyber Stability (2019)**	**Other Sources**
					expression and access to information online." NETmundial Multistakeholder Statement (2014): "Human rights are universal as reflected in the Universal Declaration of Human Rights and that should underpin Internet governance principles. Rights that people have offline must also be protected online, in accordance with international human rights legal obligations, including the International Covenants on Civil and Political Rights and Economic, Social and Cultural Rights, and the Convention on the Rights of Persons with Disabilities;"
Cooperating against Cyber Threats	**¶13(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" **¶13(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	**¶2(4):** participating States pledge "to cooperate in combating criminal and terrorist activities that use information and communications technologies and information and communications networks, and in curbing the dissemination of information that incites terrorism, separatism or extremism or that inflames hatred on ethnic, racial or religious grounds" **¶2(9):** "All States must cooperate fully with other interested parties in encouraging a deeper understanding by all elements in society, including the private			UN General Assembly Resolution 57/239 (2003) **Annex part (c)**: "Participants should act in a timely and cooperative manner to prevent, detect and respond to security incidents. They should share information about threats and vulnerabilities, as appropriate, and implement procedures for rapid and effective cooperation to prevent, detect and respond to security incidents. This may involve cross-border information-sharing and cooperation." OSCE Confidence Building Measures (2016), Nos 2 and 14: "2. Participating States will voluntarily facilitate co-operation among the competent national bodies and exchange of information in relation with security of and in the use of ICTs…. 14. Participating States will, on a voluntary basis and consistent with national legislation, promote public-private partnerships and develop mechanisms to exchange best practices of responses to common security challenges stemming from the use of ICTs." African Union Convention on Cyber Security and Personal Data Protection (not yet in force) **Art. 27(2):** "Each State Party shall adopt such measures as

Comparing Cyber Norms Across Processes					
Issue	**UN Group of Governmental Experts (GGE) Consensus Report (2015)**	**Shanghai Cooperation Organization (SCO) Code of Conduct (Revised, 2015)**	**Paris Call for Trust & Security in Cyberspace (2018)**	**Global Commission on Cyber Stability (2019)**	**Other Sources**
	measures to address such threats. States may need to consider whether new measures need to be developed in this respect" **¶35**: "While States have a primary responsibility for maintaining a secure and peaceful ICT environment, effective international cooperation would benefit from identifying mechanisms for the participation, as appropriate, of the private sector, academia and civil society organizations."	sector and civil-society institutions, of their responsibility to ensure information security, by means including the creation of a culture of information security and the provision of support for efforts to protect critical information infrastructure" **¶2(12):** Participating States pledge "[t]o bolster bilateral, regional and international cooperation, promote a prominent role for the United Nations in areas such as . . . qualitative improvements in international cooperation in the field of information security; and to enhance coordination among relevant international organizations"			it deems necessary in order to establish appropriate institutions to combat cyber-crime, ensure monitoring and response to incidents and alerts, national and cross-border coordination of cyber-security problems, as well as global cooperation." G7 Foreign Ministers' Communiqué (2018**) ¶42**: "We reaffirm our commitment to contribute to international cooperative action by working together to develop measures aimed at preventing, deterring, discouraging and countering malicious cyber acts . . . We recognize the importance of working with the private sector and civil society in addressing these challenges." Cybersecurity Tech Accord (2018) **principle 4:** "WE WILL PARTNER WITH EACH OTHER AND WITH LIKEMINDED GROUPS TO ENHANCE CYBERSECURITY. We will work with each other and will establish formal and informal partnerships with industry, civil society, and security researchers, across proprietary and open source technologies to improve technical collaboration, coordinated vulnerability disclosure, and threat sharing, as well as to minimize the levels of malicious code being introduced into cyberspace."
Supporting Capacity Building	**¶19:** "States bear primary responsibility for national security and the safety of their citizens, including in the ICT environment, but some States may lack sufficient capacity to protect their ICT networks.	**¶2(11):** Participating States Pledge "[t]o assist developing countries in their efforts to enhance capacity-building on information security and to close the digital divide"	**Principle 9**: Signatories affirm willingness to work together to "[p]romote… confidence-building measures in cyberspace.		Cybersecurity Tech Accord (2018) **principle 3:** "We will support civil society, governments and international organizations in their efforts to advance security in cyberspace and to build cybersecurity capacity in developed and emerging economies alike."

Comparing Cyber Norms Across Processes					
Issue	**UN Group of Governmental Experts (GGE) Consensus Report (2015)**	**Shanghai Cooperation Organization (SCO) Code of Conduct (Revised, 2015)**	**Paris Call for Trust & Security in Cyberspace (2018)**	**Global Commission on Cyber Stability (2019)**	**Other Sources**
	A lack of capacity can make the citizens and critical infrastructure of a State vulnerable or make it an unwitting haven for malicious actors. International cooperation and assistance can play an essential role in enabling States to secure ICTs and ensure their peaceful use. Providing assistance to build capacity in the area of ICT security is also essential for international security, by improving the capacity of States for cooperation and collective action. The Group agreed that capacity-building measures should seek to promote the use of ICTs for peaceful purposes."				
Commercial Cyber-Espionage			**Principle 4**: Signatories affirm willingness to work together to "[p]revent ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing		G20 Antalya Summit Leader's Communique, (2015), **¶26**: "...we affirm that no country should conduct or support 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 sectors;" G7 Declaration on Responsible States Behavior in Cyberspace (2017) (quoting 2015 G20 Communique ¶26) "Common understanding" between the United States and the People's Republic

Comparing Cyber Norms Across Processes					
Issue	**UN Group of Governmental Experts (GGE) Consensus Report (2015)**	**Shanghai Cooperation Organization (SCO) Code of Conduct (Revised, 2015)**	**Paris Call for Trust & Security in Cyberspace (2018)**	**Global Commission on Cyber Stability (2019)**	**Other Sources**
			competitive advantages to companies or commercial sector"		of China (Sept. 2015): "I can announce that our two countries have reached a common understanding … We've agreed that neither the U.S. or the Chinese government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information for commercial advantage."
Peaceful Settlement of Disputes	**¶2**: Reiterating, "that it is in the interest of all States to promote the use of ICTs for peaceful purposes and to prevent conflict arising from their use." **¶28(b):** "In their use of ICTs, States must observe, among other principles of international law… the settlement of disputes by peaceful means and non-intervention in the internal affairs of other States."	**¶2(13):** Participating States pledge "[t]o settle any dispute resulting from the application of this code of conduct through peaceful means, and to refrain from the threat or use of force."			European Parliament Resolution (2018/2004(INI)) (2018) **cl. 48**: Parliament "[c]onfirms its full commitment to an open, free, stable and secure cyber space . . . where international disputes are settled by peaceful means on the basis of the UN Charter and principles of international law;"
Restricting Private Hack-Backs			**Principle 8**: Signatories affirm willingness to work together to "[t]ake steps to prevent non-State actors, including the private sector, from hacking-back, for their own purposes or those of other non-State actors."	**Norm 8**: "Non-state actors should not engage in offensive cyber operations and state actors should prevent or respond to such activities if they occur."	Cybersecurity Tech Accord (2018), **principle 2**: "WE WILL OPPOSE CYBERATTACKS ON INNOCENT CITIZENS AND ENTERPRISES FROM ANYWHERE. We will protect against tampering with and exploitation of technology products and services during their development, design, distribution and use. We will not help governments launch cyberattacks against innocent citizens and enterprises from anywhere."
Preventing the Proliferation of			**Principle 5**: Signatories affirm		Wassenaar Arrangement (2017): "In 2017 WA Participating States . . .

Comparing Cyber Norms Across Processes					
Issue	**UN Group of Governmental Experts (GGE) Consensus Report (2015)**	**Shanghai Cooperation Organization (SCO) Code of Conduct (Revised, 2015)**	**Paris Call for Trust & Security in Cyberspace (2018)**	**Global Commission on Cyber Stability (2019)**	**Other Sources**
Malicious Cyber Tools and Techniques			willingness to work together to "[d]evelop ways to prevent the proliferation of malicious ICT tools and practices intended to cause harm"		adopted new export controls in a number of areas, including . . . technology related to intrusion software . . ." Charter of Trust for a Secure Digital World (2018) **principle 3**: "Security by default | Adopt the highest appropriate level of security and data protection and ensure that it is preconfigured into the design of products, functionalities, processes, technologies, operations, architectures, and business models."
Promoting Cyber Hygiene			**Principle 7**: Signatories affirm willingness to work together to "[s]upport efforts to strengthen an advanced cyber hygiene for all actors"	**Norm 7**: "States should enact appropriate measures, including laws and regulations, to ensure basic cyber hygiene."	African Union Convention on Cyber Security and Personal Data Protection (not yet in force) **Art. 26(1)(a):** "Each State Party undertakes to promote the culture of cyber security among all stakeholders, namely governments, enterprises and the civil society, which develop, own, manage, operationalize and use information systems and networks…"
Exercising Due Diligence	**¶13(c):** "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs"	**¶2(6):** Participating States pledge "To reaffirm the rights and responsibilities of all States, in accordance with the relevant norms and rules, regarding legal protection of their information space and critical information infrastructure against damage resulting from threats, interference, attack and sabotage"			
Maintaining International Peace & Security	**¶2:** "An open, secure, stable, accessible and peaceful ICT environment is essential for all and	**¶2(2):** Participating States pledge "[n]ot to use information and communications technologies and			

Comparing Cyber Norms Across Processes					
Issue	**UN Group of Governmental Experts (GGE) Consensus Report (2015)**	**Shanghai Cooperation Organization (SCO) Code of Conduct (Revised, 2015)**	**Paris Call for Trust & Security in Cyberspace (2018)**	**Global Commission on Cyber Stability (2019)**	**Other Sources**
	requires effective cooperation among States to reduce risks to international peace and security."	information and communications networks to carry out activities which run counter to the task of maintaining international peace and security."			
A Duty to Assist	**¶13(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"				Cybersecurity Tech Accord (2018), **principle 1**: "1. WE WILL PROTECT ALL OF OUR USERS AND CUSTOMERS EVERYWHERE. We will strive to protect all our users and customers from cyberattacks – whether an individual, organization or government – irrespective of their technical acumen, culture or location, or the motives of the attacker, whether criminal or geopolitical."
Attribution and Consequences	**¶13(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" **¶28(f):** "States must meet their international				G7 Foreign Ministers' Communiqué (2018), **¶42:** "We reaffirm our commitment to contribute to international cooperative action by working together to develop measures aimed at preventing, deterring, discouraging and countering malicious cyber acts and thus strengthen our collective resolve to deter malicious cyber actors by imposing costs in a timely manner. When appropriate, we will consider attributing malicious behaviour and taking action. We recognize the importance of working with the private sector and civil society in addressing these challenges;"

Comparing Cyber Norms Across Processes					
Issue	**UN Group of Governmental Experts (GGE) Consensus Report (2015)**	**Shanghai Cooperation Organization (SCO) Code of Conduct (Revised, 2015)**	**Paris Call for Trust & Security in Cyberspace (2018)**	**Global Commission on Cyber Stability (2019)**	**Other Sources**
	obligations regarding internationally wrongful acts attributable to them under international law. However, the indication that an ICT activity was launched or otherwise originates from the territory or the ICT infrastructure of a State may be insufficient in itself to attribute the activity to that State. The Group noted that the accusations of organizing and implementing wrongful acts brought against States should be substantiated."				
Pursuing Confidence Building Measures	**¶16**: "… To enhance trust and cooperation and reduce the risk of conflict, the Group recommends that States consider the following voluntary confidence-building measures . . . (b) The development of and support for mechanisms and processes for bilateral, regional, subregional and multilateral consultations, as appropriate, to enhance inter-State	**¶2(10):** Participating States pledge "[t]o develop confidence-building measures aimed at increasing predictability and reducing the likelihood of misunderstanding and the risk of conflict. Such measures will include, inter alia, voluntary exchange of information regarding national strategies and organizational structures for ensuring a State's			

Comparing Cyber Norms Across Processes					
Issue	**UN Group of Governmental Experts (GGE) Consensus Report (2015)**	**Shanghai Cooperation Organization (SCO) Code of Conduct (Revised, 2015)**	**Paris Call for Trust & Security in Cyberspace (2018)**	**Global Commission on Cyber Stability (2019)**	**Other Sources**
	confidence-building and to reduce the risk of misperception, escalation and conflict that may stem from ICT incidents …" [note: this is one of several concrete CBMs recommended by the 2015 Report).	information security, the publication of white papers and exchanges of best practice, wherever practical and advisable"			
Promoting International Norms			**Principle 9**: Signatories affirm willingness to work together to "[p]romote the widespread acceptance and implementation of international norms of responsible behavior …"		UN General Assembly Resolution 70/237 (2015): "Welcoming the conclusion of the Group of Governmental Experts in its 2013 report that . . . voluntary and non-binding norms, rules and principles of responsible behaviour of States in the use of information and communications technologies can reduce risks to international peace, security and stability, and that, given the unique attributes of such technologies, additional norms can be developed over time," G7 Declaration on Responsible States Behavior in Cyberspace (2017): "We are committed to promoting a strategic framework for conflict prevention, cooperation and stability in cyberspace, consisting of the recognition of the applicability of existing international law to State behavior in cyberspace, the promotion of voluntary, non-binding norms of responsible State behavior during peacetime, and the development and the implementation of practical cyber confidence building measures (CBMs) between States; …"
Establishing and Respecting Computer Emergency	**¶13(k):** States should not conduct or knowingly support activity to harm the information systems				

Comparing Cyber Norms Across Processes					
Issue	**UN Group of Governmental Experts (GGE) Consensus Report (2015)**	**Shanghai Cooperation Organization (SCO) Code of Conduct (Revised, 2015)**	**Paris Call for Trust & Security in Cyberspace (2018)**	**Global Commission on Cyber Stability (2019)**	**Other Sources**
Response Teams	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. **¶17(c):** "States should consider additional confidence-building measures …" including via agreements by States to "Establish a national computer emergency response team and/or cybersecurity incident response team or officially designate an organization to fulfil this role. States may wish to consider such bodies within their definition of critical infrastructure. States should support and facilitate the functioning of and cooperation among such national response teams and other authorized bodies"				