Microsoft

PROTECTING PEOPLE IN CYBERSPACE: The Vital Role of the United Nations in 2020

BACKGROUND

The United Nations this year launched two important initiatives on cybersecurity, a Group of Governmental Experts (GGE), wherein representatives of 25 countries will focus on "advancing responsible State behaviour in cyberspace,"[1] and an Open Ended Working Group (OEWG), open to all Member States as well as a limited number of non-governmental actors.[2]

Microsoft is encouraged that the United Nations (UN) has organized the first-ever multistakeholder cybersecurity conference with industry, non-governmental organizations, and academia. The conference is set to take place at UN Headquarters from December 2-4. We are honored to be among the participants and look forward to contributing to the discussion. This paper outlines our thinking on issues relevant to the conference.

SUMMARY

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.

The UN's GGE and OEWG can draw on existing work, notably the GGE's 2013 and 2015 reports that represent a global cybersecurity normative baseline.[3] This work has built on long traditions shaping how countries work together. In the last few years, respected and inclusive initiatives, such as the *Paris Call for Trust and Security in Cyberspace*[4] and the *Global Commission on Stability in Cyberspace*[5] have developed additional ideas for protecting people and their daily lives in cyberspace. Those efforts rest on expert, representative, and widely accepted analysis, and the UN can further expand the reach of their conclusions. This would be consistent with the development of international cooperation and rules in many sectors. Activities in cyberspace, which began as a self-regulated environment, will come under the auspices of more formal rules, just as has happened with activities at sea, near the Earth's poles, or in outer space — all examples of UN leadership in global governance.

This paper describes the current threat landscape in cyberspace and offers to make available our conclusions to the UN processes. It then notes that several possible norms — having to do with protecting core governmental functions and the operation of the internet itself— have wide endorsement and could benefit from consideration and acceptance by the GGE and the OEWG.

1. https://www.un.org/disarmament/group-of-governmental-experts/
2. https://www.un.org/disarmament/open-ended-working-group/
3. https://undocs.org/A/68/98; https://undocs.org/A/70/174
4. https://pariscall.international/en/
5. https://cyberstability.org/report

EXISTING AND POTENTIAL CYBER THREATS

Both UN processes properly start with an effort to understand the threat landscape today. Simply put, threats are growing as more states invest in cyber-weapons and non-state actors quickly obtain capabilities. We see this firsthand every day at Microsoft, where our Microsoft Threat Intelligence Center (MSTIC)[6] and other security teams work to analyze trillions of signals to identify sophisticated threats and protect our customers from a diverse and growing number of nation-state actors.

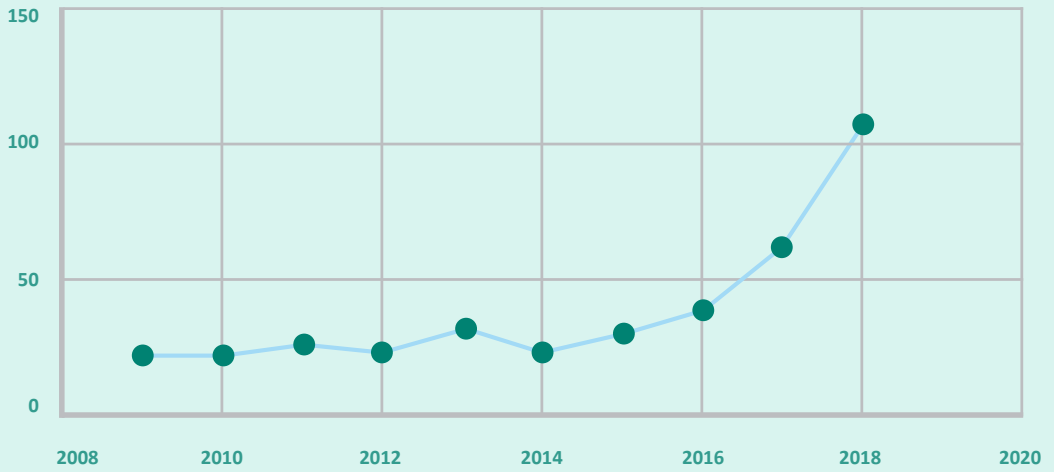
Data from the Centre for Strategic and International Studies illustrates just how dramatically the number of sophisticated cyberattacks has increased over the last decade[7] in the chart below.

The situation will continue to deteriorate if no action is taken. More than 60 nations are now developing cyber-offensive capabilities.[8] Moreover, cyber-weapons proliferate quickly when they are stolen, sold, or otherwise repurposed to criminal ends.

Digital economies require a safe, open, and secure internet. At the same time, the critical infrastructure that underpins key aspects of everyday life has become more vulnerable to evolving cyber threats. State actors have successfully disabled public access to electricity in rival countries[9] and have reportedly targeted adversaries' power grids by implanting malware as a latent threat that can be triggered at their discretion.[10] Attacks on municipal governments in the United States and Canada have threatened the functioning of everyday services, and efforts to infiltrate electoral processes, including voter rolls and the tabulation of votes, have been widely reported. Such attacks may also have indiscriminate or unintended effects, as when an attack on computer systems in Ukraine impeded a global shipping company based in Denmark and many other infrastructures around the world.

Significant Cyber Incidents (2009-2018)

Based on data in the CSIS report "Significant Cyber Incidents Since 2006"



OEWG/GGE BRIEFINGS FROM THE PRIVATE SECTOR AND CIVIL SOCIETY

Because private sector and civil society organizations are often responsible for providing individuals and organizations with a secure, open, and functioning internet as well as key applications and services, they often have unique and deep understanding of threats in cyberspace. The Microsoft Threat Intelligence Center (MSTIC) has focused on tracking the malicious activities carried out by the most sophisticated state actors for more than a decade. In pursuing this work, our security researchers have been able to observe trends in tactics, techniques, and processes. We would welcome the opportunity to provide information we have, to the extent legally possible, to the UN processes. We believe that other organizations with expertise in this area would also welcome this opportunity.

6. https://www.microsoft.com/en-us/security/operations/intelligence

7. *Significant Cyber Incidents Since 2006*. CSIS. https://csis-prod.s3.amazonaws.com/s3fs-public/190904_Significant_Cyber_Events_List.pdf

8. Valantino-DeVries, Jenniter, Lam Thuy Vo, Danny Yadron. *Cataloging the World's Cyberforces*. Wall Street Journal. http://graphics.wsj.com/world-catalogue-cyberwar-tools/

9. Greenberg, Andy. *How An Entire Nation Became Russia's Test Lab for Cyberwar.* Wired. June 20, 2017. https://www.wired.com/story/russian-hackers-attack-ukraine/

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

SUGGESTIONS FOR PROTECTION OF PEOPLE IN CYBERSPACE

The Role of International Law & How it Applies to Cyberspace

Discussions about the role of international law have been part of UN cybersecurity discussions since 1998. In the 2013 GGE report, 15 states' representatives agreed that (a) international law, including the UN Charter, applies to Information and Communication Technologies (ICT); and (b) applying that law is "essential" to maintaining peace and stability, and an "open, secure, peaceful and accessible ICT environment."[11] The 2015 GGE report reiterated these conclusions and went a step further, offering a non-exhaustive list of *how* international law applies, including by (i) granting states jurisdiction over ICT infrastructure in their territory; (ii) directing states to observe principles of sovereignty, sovereign equality, peaceful settlement of disputes, non-intervention, and human rights; (iii) referencing International Humanitarian Law (IHL) principles (albeit without endorsing IHL's application explicitly); and (iv) prohibiting states from using proxies to violate international law via ICTs.[12]

The sixth iteration of the GGE will continue to study this issue while inviting "national contributions" on how international law applies to ICTs. Meanwhile, the OEWG seeks to make UN processes "more democratic, inclusive, and transparent" — with a mandate to (i) review previous GGE outputs and "if necessary, to introduce changes to them or elaborate on additional rules of behaviour"; (ii) continue to study how international law applies to the ICT environment; and (iii) solicit views from non-state stakeholders on issues within the OEWG mandate.

Since the 2013 and 2015 GGE reports, other Member State organizations, including ASEAN, NATO and the EU, have affirmed international law's application to cyberspace. Several states, including Estonia,[13] France,[14] and the United Kingdom,[15] have gone further, offering official statements on how they understand international law applies. Scholars have made similar efforts, most prominently through the two *Tallinn Manuals* funded by the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE).

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. 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 the safety, security, and trust of individuals and organizations.

Given current trends, it is clear that international law either (a) does not sufficiently prohibit some of the most egregious and unwanted cyberactivity, 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 or deterrence of or consequences for unwanted activity.

To address this, Microsoft has encouraged the development of clear and binding legal obligations for cyberspace — what has been called a *Digital Geneva Convention*. However, regardless of whether a separate treaty is pursued, the following are discrete recommendations for how the GGE and OEWG may work to strengthen existing commitments as well as address key "grey areas" in international law:

11. https://undocs.org/A/68/98

12. https://undocs.org/A/70/174

13. Kaljulaid, Kersti, President of Estonia. Opening Remarks at CyCon 2019. May 29, 2019. https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html

14. Ministère des Armées. Droit international appliqué aux operations dans le cyberspace. September 9, 2019. https://www.defense.gouv.fr/salle-de-presse/communiques/communiques-du-ministere-des-armees/communique_la-france-s-engage-a-promouvoir-un-cyberespace-stable-fonde-sur-la-confiance-et-le-respect-du-droit-international

15. Wright, Jeremy. Cyber and International Law in the 21st Century. May 23, 2018. https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century

BUILD UPON EXISTING 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 upon this foundation, recognizing the authority of international law, including the rights of states granted by the UN Charter. Microsoft encourages the current UN cyber dialogues to further confirm the applicability of existing international law regimes to cyber operations. This application of international law specifically includes:

International Humanitarian Law (IHL), which includes the qualification that cyber operations targeting only data can be considered "attacks" to which its various principles — distinction, proportionality, necessity — still apply.

Due diligence, which involves holding a state liable for transboundary harms caused by malicious cyber activities originating in its territory and 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, including 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.

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.

Human Rights including the need to protect freedom of speech without facilitating violent online extremist behavior.

ENCOURAGE INCREASED TRANSPARENCY BY STATES

Microsoft encourages the UN dialogues to promote and facilitate efforts to enable *all* UN Member States to produce official positions on how international law applies in cyberspace, helping 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 UN cyber dialogues 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.

Rules, Norms & Principles for Cyberspace

STRENGTHEN SUPPORT FOR EARLIER GGE REPORTS

Earlier GGE processes issued important norms of responsible state behavior online, asserting the applicability of international law to cyberspace and establishing: protections for critical infrastructure, computer emergency response teams, and human rights; prohibitions against the use of cyberspace for activities that violate international law; and commitments to responsibly disclose ICT vulnerabilities and ensure the integrity of ICT supply chains. These have been endorsed by the General Assembly and thus have wide support. This 6th GGE and the OEWG can build upon these conclusions, reinforcing the status of these important norms.

ENDORSE EMERGING NORMS FOR PROTECTION IN CYBERSPACE

The OEWG and GGE might identify which of these have support among a substantial number of states and whether any of these principles and norms — as yet non-binding even for states that have endorsed them — are seen as reflecting international law in the opinion of states that submit views. If these norms are regarded as binding, then customary international law may be emerging in cyberspace; if they are seen as non-binding, then it may be necessary to pursue a legally binding instrument.

In the years since the landmark 2015 GGE report, and even while the 2017 GGE could not reach agreement on issuing a consensus report, progress on norms development has continued. While we do not believe a significant number of new norms are needed, we suggest the GGE and OEWG endorse *three important principles* that have emerged from diverse, representative, and expert discussions among states and other stakeholders:

Cyberspace for everyday purposes should be protected from cyberattacks. This principle reflects the growing importance – and vulnerability – of cyberspace as it becomes more critical to everyday life. International law, as previous GGEs and an increasing number of states have recognized, applies in cyberspace. This recognition, however, leaves several important gaps in what activities are protected. According to existing international humanitarian law, during a time of war, everyday activities would largely be protected from attacks, whether targeted or indiscriminate in nature. It is difficult to justify a situation in which an attack that would be forbidden during times of war would be acceptable in peacetime. As such, a critical principle to consider as a new norm is a prohibition against cyberattacks that cause significant, indiscriminate, or systemic harm to people or civilian infrastructure at any time.

Electoral processes should be protected from malicious foreign interference through cyberattacks. The ability of a people to select its leaders without foreign interference is a core element of sovereignty, as well as a component in allowing for self-determination and political independence — central pillars of the UN Charter. Since the 2015 GGE report, diverse and expert international groups have identified the importance of a specific norm protecting electoral processes.

Chief among these initiatives were the Paris Call for Trust and Security in Cyberspace,[16] announced by President Macron in 2018, and the Global Commission on the Stability of Cyberspace (GCSC).[17] The Paris Call's nine voluntary principles, including a prohibition against malign foreign interference in elections through malicious cyber activities, comprise the most widely endorsed multistakeholder commitment on responsible behavior in cyberspace. More than 1000 supporters, including 75 governments and hundreds of civil society and industry organizations, have endorsed the Paris Call. The GCSC, a multinational body of experts drawn from government, academia, civil society, and the private sector has similarly released eight norms, including a protection for technical infrastructure essential to elections. Other leading global and regional state-led bodies, including the G7, have issued declarations against malign foreign interference in electoral processes.

Elements central to the functioning of the internet should be protected. As the internet becomes more entwined with daily life, it is ever more important that it remain secure, stable, and safe. Previous GGE commitments reflect this importance, and various statements since, including the Paris Call and the GCSC, reflect growing commitment to protect the technology that constitutes the backbone of internet itself from cyberattacks. Some efforts refer to this as protecting the general availability or integrity of the "public core"[18] of the Internet, with some preferring reference to technical components of the internet. Importantly, states should agree on a new norm to protect those central components without which the global Internet would cease to operate. The GCSC defines these components as: packet routing and forwarding; naming and numbering systems; cryptographic mechanisms of security and identity; transmission media, software and data centers.

16. The Paris Call for Trust and Security in Cyberspace, https://pariscall.international/en/

17. The Global Commission for the Stability of Cyberspace, https://cyberstability.org/

18. GCSC Norm on Protecting the Public Core of the Internet, https://cyberstability.org/norms/#toggle-id-1

ACCOUNTABILITY & ADHERENCE TO NORMS

While valuable, efforts to reaffirm existing norms and adopt a limited set of new norms by themselves will not be sufficient to truly protect people and infrastructure in cyberspace. Microsoft strongly encourages the OEWG and GGE to consider the need to:

Highlight norms violations. The attribution of a cyberattack to a state that is in violation of international norms should always include an explicit and direct articulation of which norm was transgressed and how. Where reasonable, greater transparency in the underlying information used in drawing those conclusions will lend the attribution greater credibility and further strengthen the recognition of norms.

Establish deterrence doctrines. Rather than further escalating tensions, clear doctrines of measured consequences for cyberattacks in violation of international agreements will help deter further belligerence, as well as provide necessary clarity about what responses can be expected. The European Union recently led the way in this regard in the establishment of a sanctions' regime aimed at deterring cyberattacks.[19]

Multilateral consequences. Beyond deterrence doctrines established by individual nations or coalitions, the international community as a whole should pursue the establishment of clear, non-escalatory consequences for violations of established norms, rules, and principles through existing forums and structures, such as those at the UN or World Trade Organization (WTO). The United States and numerous other countries recently agreed on increased coordination on holding accountable nation-states that violate agreed-upon norms.[20]

INSTITUTIONAL DIALOGUE

ESTABLISH REGULAR MULTISTAKEHOLDER CONSULTATIONS

Cyberspace is a shared domain, and norms governing it will be most effective if they rest on the shared experience of all stakeholders. The UN should seek to establish ways for stakeholders from civil society and the private sector to play a role in discussing the cyber environment and norms for behavior in it.

IMPLEMENT THE UN HIGH-LEVEL PANEL FOR DIGITAL COOPERATION RECOMMENDATIONS

One important opportunity to advance more regular multistakeholder consultations on these issues may be through implementation of the recommendations set forth in the *UN Secretary General's High-Level Panel on Digital Cooperation*.[21] As the UN explores next steps, the Panel's Recommendation 4 for a Global Commitment on Digital Trust and Security and its Recommendation 5 on Global Digital Cooperation could play a meaningful role in advancing international peace and security and should be a focal point for all Member States.

CONFIDENCE BUILDING MEASURES (CBMS)

Trust is at the foundation of any meaningful interaction between different parties. In an interaction between parties that have previously been engaged in conflict, the importance of trust is further amplified though often difficult to achieve. *Confidence Building Measures* (CBMs) are a key tool for building trust, including in the context of cybersecurity, and can include: voluntary exchange of information, such as military doctrine or capabilities; and establishment of direct "hot-lines" between senior political leaders to enhance communication and reduce the risk of misperception between nations. Notable agreements in this realm include two sets of cybersecurity CBMs agreed to by Member States of the *Organization for Security and Co-operation in Europe* (OSCE).[22]

19 Cyber-attacks: Council is now able to impose sanctions. European Council. May 17, 2019. https://www.consilium.europa.eu/en/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/

20. Joint Statement on Advancing Responsible Behavior in Cyberspace, U.S. Department of State, September 20, 2019 https://nz.usembassy.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/

21. Overview of the UN Secretary-General's High-Level Panel on Digital Cooperation

22. OSCE Statement on Expanded ICT Confidence Building Measures, March 10, 2016 https://www.osce.org/cio/226656

FOCUS ON IMPLEMENTATION OF CBMS

Microsoft has provided an industry perspective to a number of CBMs discussions, including those at the OSCE as well as the European Union (EU), the Organization of American States (OAS), the ASEAN Regional Forum (ARF), and the UN. We encourage the OEWG and GGE to further build on the work in these fora to date to create opportunities for additional confidence building measures and — importantly — focus on implementation of CBMs by providing resources, best practices and (where applicable) funding to less developed states. Moreover, we encourage Member States to tap into significant technical and organizational experience in the private sector and civil society to help ensure that CBMs are developed and implemented with multistakeholder input.

CYBERSECURITY CAPACITY BUILDING

Cybersecurity capacity building was recognized in the 2013 GGE report, which described it as bridging uneven levels of security and developing relevant skills and adequate institutional frameworks. Concurrently, the importance of cybersecurity capacity building was also recognized as part of the London Process.

The resulting Global Conferences on Cyberspace featured capacity building prominently, which led in 2015 to the creation of the Global Forum on Cyber Expertise (GFCE),[23] a global platform for countries, international organizations, and private companies to exchange best practices and expertise on cybersecurity capacity building.

THE OEWG AND THE GGE SHOULD STRONGLY SUPPORT CAPACITY BUILDING

Both the OEWG and the GGE have the potential to positively impact the security and stability of cyberspace by promoting cybersecurity capacity building. Norms and confidence building measures will only be effective if Member States have the capability and capacity to meaningfully implement them. With that in mind, Microsoft encourages Member States to:

Utilize existing mechanisms. Numerous states, foundations, and private actors have dedicated funding and resources to capacity building initiatives. Instead of replicating those efforts, Microsoft encourages Member States to pool resources to generate greater impact, and participate in fora, such as the *Global Forum for Cyber Expertise*, which can help match needs with expertise.

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 an understanding of where they have gaps in capacity or capability. Inevitably, these needs will vary depending on regional or local context.

Strengthen cyber diplomacy. All too often, capacity building efforts focus on the technical aspects of cybersecurity — which are necessary but not enough. One aspect 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.

Be inclusive of all stakeholders. It is critical that capacity building focus not just on government stakeholders but industry and civil society as well. Multistakeholder perspectives should thus be included in relevant trainings, exercises, and other cybersecurity capacity building actions.

23. Global Forum on Cyber Expertise. https://www.thegfce.com/

CONCLUSION

The OEWG and the GGE are important initiatives that must succeed in their missions. Microsoft welcomes the opportunity to provide its views and experience along with others from civil society and the private sector.

We are strong supporters of robust cybersecurity norms, which must build on the primacy of international law and its application to cyberspace.

We encourage UN Member States to explore strengthening multistakeholder processes and platforms for sustained dialogue on the use of information and communication technologies in the context of international peace and security.

We support and stand ready to help advance confidence building measures in cyberspace and capacity building efforts to help create a common global cybersecurity baseline.

Our suggestions are intended to provide a perspective from one particular vantage point but also to underscore the urgency — which is reflected by the establishment of these two groups — of providing effective protection in cyberspace. We stand ready and look forward to engaging in further dialogue on these important issues with both the OEWG and the GGE as well as individual Member States, companies, and civil society organizations.

For feedback, please contact:
protectcyberspace@microsoft.com