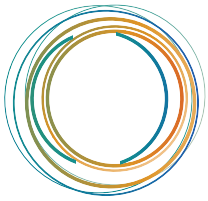
accessnow

A DIGITAL RIGHTS APPROACH TO THE TECH ACCORD AND THE DIGITAL GENEVA CONVENTION

September 2018

accessnow.org



Access Now defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.

accessnow

TABLE OF CONTENTS

I. INTRODUCTION

Nation state cybersecurity operations, including government hacking, are causing escalating damage to societies around the world. We are seeing a strategy of "securitization," where state authorities use the internet for operations that can cause permanent damage to internet infrastructure and inflict harm on users, who have little or no recourse. This is happening largely in the absence of norms to govern government or corporate behavior, with states leveraging their legitimacy and dedicated resources to carry out objectives that erode human rights on a broad scale.

Some private companies are facilitating dangerous, unpredictable, and largely opaque state cyber operations, either by developing the underlying technology to support them, or by ceding to government demands despite their responsibility to respect human rights. Government-led attempts to reduce the harm of these operations, meanwhile, have had only limited success.[1]

However, a number of leading technology companies have begun to work together to address these issues, launching the Cybersecurity Tech Accord (Tech Accord) and the Digital Geneva Convention (DGC).

The principles advanced through the Tech Accord and DGC can help to establish badly needed international norms, including several that we support at Access Now.[2] However, we believe both initiatives can be even stronger, both in terms of structure and content. Importantly, neither one should downplay the rule of law or sidestep the international human rights framework. To the contrary, they should serve to reinvigorate and reinforce existing human rights commitments, both by companies and governments.

Access Now advocates for cybersecurity policy that is built on global human rights standards, and our policy guidance for state hacking is likewise built on these standards.[3] In this response paper, we offer recommendations to improve the Tech Accord and the DGC, including by integrating these initiatives within the human rights framework.

We encourage the companies that have signed the Tech Accord to further develop their commitments, and for Microsoft to continue supporting the development of global standards for attribution of cyber attacks. We also support the discussion surrounding the DGC proposal, as the initiative has the potential to generate positive norms. We stand ready to facilitate making improvements to better protect the end users and defend their fundamental rights.

[1] https://www.cfr.org/interactive/cyber-operations
[2] See e.g. https://www.accessnow.org/policy-makers-guide-global-conference-cyberspace-2017/
[3] https://www.accessnow.org/cms/assets/uploads/2017/11/A-Policy-Makers-Guide-to-GCCS-2017-digital-v.pdf; https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf

II.
A CLOSER LOOK AT THE TECH ACCORD AND DIGITAL GENEVA CONVENTION PROPOSALS

TECH ACCORD

The Tech Accord is "a public commitment among more than 30 global companies to protect and empower civilians online and to improve the security, stability, and resilience of cyberspace."[4] Microsoft initially designated six common objectives as the basis for an accord, which included emphasizing incident response. In April of 2018, 34 companies in the U.S. and Europe signed and published the Tech Accord, "agreeing to defend all customers everywhere from malicious attacks by cybercriminal enterprises and nation-states." The accord has **four principles**, summarized online:

- **Stronger defense**
  The companies will mount a stronger defense against cyberattacks. As part of this, recognizing that everyone deserves protection, the companies pledged to protect all customers globally regardless of the motivation for attacks online.

- **No offense**
  The companies will not help governments launch cyberattacks against innocent citizens and enterprises, and will protect against tampering or exploitation of their products and services through every stage of technology development, design, and distribution.

- **Capacity building**
  The companies will do more to empower developers and the people and businesses that use their technology, helping them improve their capacity for protecting themselves. This may include joint work on new security practices and new features the companies can deploy in their individual products and services.

- **Collective action**
  The companies will build on existing relationships and together establish new formal and informal partnerships with industry, civil society, and security researchers to improve technical collaboration, coordinate vulnerability disclosures, share threats, and minimize the potential for malicious code to be introduced into cyberspace.

DIGITAL GENEVA CONVENTION

According to Microsoft, the purpose of the DGC[5] is to:

> "commit governments to protecting civilians from nation-state attacks in times of peace. And just as the Fourth Geneva Convention recognized that the protection of civilians required the active involvement of the Red Cross, protection against nation-state cyberattacks requires the active assistance of technology companies. The tech sector plays a unique role as the internet's first responders, and we therefore should commit ourselves to collective action that will make the internet a safer place, affirming a role as a neutral Digital Switzerland that assists customers everywhere and retains the world's trust."

The DGC consists of a series of principles summarized in the blog post and provided with more detail in the position paper. **These principles** are presented below with information from both sources for clarity:

[4] https://cybertechaccord.org/
[5] https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/

II. A CLOSER LOOK AT THE TECH ACCORD AND DIGITAL GENEVA CONVENTION PROPOSALS

1. Exercise restraint in developing cyber weapons and ensure that any developed are limited, precise, and not reusable. States should also ensure that they maintain control of their weapons in a secure environment.

2. No targeting of tech companies, private sector, or critical infrastructure

- Refrain from attacking systems whose destruction would adversely impact the safety and security of private citizens (i.e., critical infrastructures, such as hospitals, electric companies).
- Refrain from attacking systems whose destruction could damage the global economy (e.g., integrity of financial transactions), or otherwise cause major global disruption (e.g., cloud-based services).
- Refrain from hacking personal accounts or private data held by journalists and private citizens involved in electoral processes.
- Refrain from using information and communications technology to steal the intellectual property of private companies, including trade secrets or other confidential business information, to provide competitive advantage to other companies or commercial sectors.
- Refrain from inserting or requiring "backdoors" in mass-market commercial technology products.

3. Assist private sector efforts to detect, contain, respond to, and recover in the face of cyberattacks. In particular, enable the core capabilities or mechanisms required for response and recovery, including Computer Emergency Response Teams (CERTs). Intervening in private sector response and recovery would be akin to attacking medical personnel at military hospitals.

4. Agree to a clear policy for acquiring, retaining, securing, using, and reporting of vulnerabilities that reflects a strong mandate to report them to vendors in mass-market products and services.

5. Agree to limit proliferation of cyber weapons. Governments should not distribute, or permit others to distribute, cyber weapons and should use intelligence, law enforcement, and financial sanctions tools against those who do.

6. Limit engagement in cyber offensive operations to avoid creating mass damage to civilian infrastructure or facilities.

Microsoft has also called for the establishment of an independent organization to investigate and attribute state responsibility for attacks, similar to the International Atomic Energy Agency, with technical experts from relevant stakeholder groups. The company published a separate paper with details on the proposed independent organization that is intended to attribute state attacks against infrastructure in order to "better deter nation-state attacks in cyberspace."[6] According to the paper, the collaboration will depend heavily on stakeholder cooperation, with support from nonprofit organizations, and sharing evidence, to determine who is responsible for attacks to steal information or harm systems. The organization will utilize "powerful analytics" and gain in-depth knowledge over time. According to the proposal, the organization would also have a mechanism to work with government experts, but not be subject to government vetoes, as it would need to be "staunchly neutral."

[6] https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QI

III.
ACCESS NOW'S RECOMMENDATIONS

In initiatives to put necessary boundaries on state cybersecurity operations, stakeholders have often downplayed the importance of human rights, and the Tech Accord and DGC are no exception. To make these two initiatives stronger and more effective in accomplishing their goals, they should each go further in addressing the rights of users, including making explicit reference to the application of existing human rights protections.

There are other areas for improvement. DGC in particular puts too much emphasis on the role of the private sector for addressing the threats posed by nation-state cybersecurity operations. Both initiatives miss the opportunity to articulate how those working under the Tech Accord or the DGC will coordinate with stakeholders such as government representatives, members of civil society, researchers, and the tech community at large. To date, the multistakeholder model for governance has been critical to the internet's success, security, and openness, including as a vehicle for the realization of a wide range of human rights. We strongly advocate that when cybersecurity policy is developed, those involved use open and pluralistic processes.

We propose the following recommendations, which we explore in detail below:

→ **1. Develop the problem definition:** Further develop the Tech Accord to clearly articulate the extent and boundaries of the problems at issue; the methods participating companies will use to address them; and how the accord interacts with existing efforts on business and human rights.
→ **2. Build out standards for attribution:** Rather than creating a centralized attribution organization, work with a broad range of stakeholders to develop a common understanding of attribution, with agreement on evidentiary standards and norms.
→ **3. Move away from the war time analogy:** Analogize to other sources of international law, including those applicable outside the law of war, to avoid perpetuating the atmosphere of conflict.
→ **4. Build cybersecurity from human rights up:** Promote a holistic view of cybersecurity that explicitly aims to protect human rights and users, includes all stakeholders as the keepers of peace and neutrality online, and articulates the responsibilities of governments outside protections applied to the private sector. Develop binding and enforceable legal mechanisms to address the inherent deficiencies of co- or self-regulatory measures around oversight and remedy for users.

1. Develop the problem definition

The companies that have signed the Tech Accord have agreed to resist nation-state and criminal attacks to protect their customers, and have taken a step toward promoting corporate respect for the human rights of their users. The Tech Accord asks global tech companies not to assist governments in offensive operations, to protect technology against tampering, and to offer products that "prioritize" privacy and security. It does not identify the harms users face from these attacks, nor does it address the proactive steps companies should take to protect users, such as implementing data security and data privacy measures that would improve accountability across sectors. The Tech Accord could serve to apply more pressure on companies to respect human rights when developing and deploying their products.

The Tech Accord does not commit the companies to participating in any particular process to promote protections for their users, such as the Freedom Online Coalition, or to assess their own efforts, like the Global Network Initiative undertakes. The companies behind the Tech Accord also have the opportunity to demonstrate the work they are already doing in this area by promoting the United Nations Guiding Principles

III. ACCESS NOW'S RECOMMENDATIONS

on Business and Human Rights, a framework that the technology sector can reinforce through innovative implementation.

- **RECOMMENDATION: Further develop the Tech Accord to clearly articulate the extent and boundaries of the problems at issue; the methods participating companies will use to address them; and how the accord interacts with existing efforts on business and human rights.**

2. Build out standards for attribution

A centralized, independent agency would face significant barriers to overcoming the practical difficulties in attributing attacks, building legitimacy, and resisting political pressures. Better attribution is necessary, although it will take time and serious consultation. The neutrality of organizations attributing attacks is essential, and that would be difficult to ensure with a unified organization tasked with global attribution. For now, attribution can be improved across a variety of active stakeholders through leadership on the development of guidelines and evidentiary standards that would enable a decentralized web of organizations to conduct attribution.

- **RECOMMENDATION: Rather than creating a centralized attribution organization, work with a broad range of stakeholders to develop a common understanding of attribution, with agreement on evidentiary standards and norms.**

3. Move away from the war-time analogy

The use of the language of armed conflict in the Tech Accord and DGC, including the explicit link the Geneva Conventions, which are intended to protect civilians in times of war, may perversely contribute to the belief that states are in a perpetual armed conflict online ("cyberwar" in military terminology) and are therefore permitted to respond in ways that may incidentally endanger internet users "in times of peace."

Employing this language — including "Geneva Convention" in particular — in the development of these norms may therefore undermine peaceful treatment and the security of the internet. The use of the term Geneva Convention serves a practical purpose: it may increase the profile of the DGC by placing it in line with a universally recognized and widely lauded agreement. Using "cyberspace" may also draw the attention of the military experts that Microsoft may see as an important audience.

However, the language of cyberwarfare is too often used to describe everyday actions that likely fall below the threshold of armed attack or a state of armed conflict under international law. Conversely, in covering peacetime, the DGC leaves unaddressed state behavior in wartime. Those distinctions matter when armed attacks and armed conflict come with their own set of rules for action that governments are permitted to take.[7] If states perceive cyberspace to be in a perpetual state of armed conflict, they may feel empowered to freely use offensive operations or to carry out traditional military responses to online threats. The states acting without restraint to launch cyber operations must be treated as acting outside the norms of state behavior.

Moreover, the current legal standards in the international human rights system already limit government threats to civilians during peacetime (as well as wartime) and cyber operations risk significant interference with fundamental human rights. In a supporting document, Microsoft called for restraint in attacks against critical infrastructure, journalists, and private citizens engaged in the electoral process.[8] While all are deserving of protection, Microsoft should clarify its aim, to emphasize that the DGC is

[7] See Tallinn Manual 2.0. https://en.wikipedia.org/wiki/Tallinn_Manual
[8] https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH.

III. ACCESS NOW'S RECOMMENDATIONS

meant to reinforce existing human rights protections in general, rather than create a new international framework. And where there are gaps in the DGC, one should look to the human rights system for answers.

There are other areas of international law, not limited to wartime, that the DGC can more appropriately analogize to, instead of the Geneva Convention. For example, in its position paper on the DGC, Microsoft addressed two arms control treaties, the Treaty on the Non-Proliferation of Nuclear Weapons and the Chemical Weapons Convention, as "examples of the international community coming together to effectively manage weapons with the potential to create catastrophic harm." Unlike the Geneva Convention, both limit state behavior at all times. The Montreux Document explains states' legal obligations and good practices toward private military and security companies during wartime.[9] Although it is applicable to states, the document also details private sector responsibilities, as "[private sector companies] are obliged to comply with international humanitarian law or human rights law imposed upon them by applicable national law." Those driving the Tech Accord and DGC could look more in depth at where and how those treaties and documents are effective and what lessons can be applied to cyber operations.

The failure of the most recent gathering of the United Nations Group of Governmental Experts (GGE) demonstrates that there are lingering divisions and conflicts of understanding in how to apply international law in the digital age.[10] Rather than working to establish an overarching treaty, it may be more effective to push receptive governments and companies on norms of responsibility, including those already agreed upon in the work of the GGE and some advanced by Microsoft, and to greater adherence to existing treaties. Once norms gain recognition and translate into common practice, codifying them internationally poses less of a challenge.

RECOMMENDATION: Analogize to other sources of international law, including those applicable outside the law of war, to avoid the perpetuating the atmosphere of conflict.

4. Build cybersecurity from human rights up

Cybersecurity norms and policies must respect and protect human rights, including the rights to privacy and freedom of expression. Those protections should enable internet users to implement digital security measures such as encryption and permit secure and anonymous communications, which are essential to the exercise of human rights online.[11] Moreover, while international law permits certain limitations and derogations to human rights during emergencies and armed conflict, those controls should only be applied narrowly so that states otherwise continue to protect and respect rights.[12]

While some key processes have failed to address the importance of human rights in cybersecurity policy-making, others, including on the international level, have recognized the necessity of a human rights-based approach to cybersecurity. The Freedom Online Coalition, a network of "countries committed to protecting and promoting online freedoms domestically and abroad," published through a working group that included

[9] https://www.icrc.org/eng/assets/files/other/icrc_002_0996.pdf.
[10] The UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security has issued three reports on norms of behavior in cyberspace and methods for states to cooperate to address those threats. While the GGE issued consensus reports in 2010, 2013, and 2013, it failed to reach consensus on a report in 2017. See https://www.un.org/disarmament/topics/informationsecurity.
[11] http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx/.
[12] See Tallinn Manual 2.0 Rules 37 and 38.

III. ACCESS NOW'S RECOMMENDATIONS

industry and civil society, "Recommendations for Human Rights Based Approaches to Cybersecurity."[13] Earlier, the Organization for Economic Co-Operation and Development (OECD) published a recommendation on "Digital Security Risk Management for Economic and Social Prosperity" that called for digital security risk management consistent with human rights and fundamental values.[14]

For example, the DGC calls for restraint in the development and use of "cyberweapons" and the Tech Accord aims to protect against "cyberattacks." If, by "cyberweapons," Microsoft means tools used to carry out government hacking efforts, the potential risks for human rights are significant. For one, Microsoft may or may not mean to address government hacking operations for the purpose of conducting surveillance or spreading propaganda, the threat of which has been raised by the OSCE Representative on Freedom of Media and others.[15] However, classifying speech as a weapon, including the speech of foreign actors, may enable restrictions on freedom of expression.

Moreover, Microsoft's call for "restraint" in use of "cyberweapons" to those that are "limited, precise, and not reusable" is valuable, but it fails to capture that even with precision such tools can be used to suppress human rights. The DGC's limitations should ensure that government restraint not only be limited but compliant with other human rights obligations, such as ensuring the necessity, proportionality, and legitimate aim of restrictions.[16] Due to the potential for serious harm, Access Now has called for a presumptive prohibition on all government hacking and greater information about the programs.[17]

The DGC and Tech Accord capture protections for the private sector effectively but miss addressing some of the most pressing threats for users. While Microsoft acknowledges that companies are often the first line of defense, protecting companies and protecting technology users is not the same in every instance. In many parts of the world, technology companies are state-owned or otherwise controlled, and therefore play a greater role in the foreign affairs and military objectives of the government. The limitations also miss the potential for nation states to infiltrate and cause damage at the user level. The call against targeting of "tech companies, private sector, and critical infrastructure" fails to protect the technology sitting on desks and in pockets. Governments use malware to target the tools used by academia, civil society, journalists, and the tech community at large without threatening the companies directly.[18] This behavior should be considered reprehensible commensurate to the harm, including those harms directed at individuals, rather than focusing on whether the attack used private-sector technology. Some states have taken steps to respond to this threat, even if imperfectly, by limiting the export of technology that can be used maliciously.

- **RECOMMENDATION: Promote a holistic view of cybersecurity that explicitly aims to protect human rights and users, includes all stakeholders as the keepers of peace and neutrality online, and articulates the responsibilities of governments outside protections applied to the private sector. Develop binding and enforceable legal mechanisms to address the inherent deficiencies of co- or self-regulatory measures around oversight and remedy for users.**

[13] https://www.freedomonlinecoalition.com/wp-content/uploads/2014/04/FOC-WG1-Recommendations-Final-21Sept-2015.pdf.
[14] https://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf.
[15] http://www.osce.org/fom/203926?download=true.
[16] https://necessaryandproportionate.org/.
[17] https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf; see https://www.ohchr.org/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf.
[18] https://www.nbcnews.com/news/latino/high-profile-lawyers-targeted-mexico-spyware-scandal-n78879

IV.
A WORD ON THE GENEVA CONVENTION AND INTERNATIONAL NORMS

THE FOURTH GENEVA CONVENTION AND THE LAW OF ARMED CONFLICT

The original Geneva Convention covered state responsibilities to civilians during war ("armed conflict" under international law) and therefore the use of its language may encourage contemplation or use of the law of armed conflict. Each new Geneva Convention addressed an emerging issue arising in this general area. Governments adopted the fourth Geneva Convention, the inspiration for the current DGC proposal, in response to the atrocities of World War II, to address attacks against civilians.[19] The DGC, however, addresses state responsibilities to civilians during peacetime, territory already covered by the 1948 Universal Declaration of Human Rights and subsequent human rights documents.[20] While the announcement of the DGC acknowledged the critical distinction between peacetime and war, that distinction may be lost as the framework is promoted.

Once triggered, an international armed conflict involves "hostilities" between two or more states.[21] International law aims to limit the harm to civilians during armed conflict. According to the experts behind the Tallinn Manual, international law prohibits attacks against users using ICTs, but permits harm, including foreseeable harm, in acting on military objectives.[22] Even civilian infrastructure — such as the technology underlying the internet — may be lawfully targeted if it qualifies as a military objective.[23] Therefore, "cyberwarfare" in the strict sense would likely look more like traditional warfare with a corresponding level of human suffering where "injury, death, damage, or destruction are intended or foreseeable."[24] According to the International Committee of the Red Cross, "cyberwarfare" on its own, not in conjunction with traditional "kinetic" operations, is theoretical and no state is known publicly to have conducted such operations.[25] Conflating the espionage, intellectual property theft, and gamesmanship commonly conducted online with warfare would have serious repercussions for internet users.

Characterization matters when it determines how a state may respond. A number of western countries have published law-of-war manuals with interpretations of their international law obligations, including in the digital realm. Those manuals demonstrate the acute risk of using the language of cyberattack and cyberwar. For example, the U.S. maintains it has broad leeway to respond to actions in self-defense with responses that need not be limited to the internet.[26]

[19] https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?documentId=AE2D398352C5B028C12563CD002D6B5C&action=openDocument.
[20] http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf.
[21] Tallinn Manual 2.0 Rule 82.2.
[22] See id Rules 92-98.
[23] Id Rule 99.
[24] https://www.icrc.org/eng/assets/files/other/365_400_schmitt.pdf at 375.
[25] https://www.icrc.org/en/document/international-humanitarian-law-and-challenges-contemporary-armed-conflicts/
[26] See https://www.defense.gov/Portals/1/Documents/pubs/Law-of-War-Manual-June-2015.pdf/ 16.3.3.1 and 16.3.3.2; The European Union has continued to put emphasis on the need for cooperation on the defense of networks and the security of infrastructure. As cross-border cyber operations fall under the auspices of traditional national security, it is not within the competence of the EU to dictate or direct its member states and their actions in this field. In Europe, the most notable steps were taken in July 2016 when NATO reaffirmed its defensive mandate and recognised cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land and at sea (http://www.nato.int/docu/review/2016/Also-in-2016/cyber-defense-nato-security-role/EN/index.htm).

IV. A WORD ON THE GENEVA CONVENTION AND INTERNATIONAL NORMS

INTERNATIONAL NORMS FOR "CYBERSPACE"

Microsoft addressed the progress of multilateral efforts to better protect cyberspace, namely the 2015 United Nations GGE report,[27] the bilateral agreement between the U.S. and China not to participate in the cyber theft of intellectual property (IP),[28] and the Group of 20 adoption of the same principle to protect IP. [29] While progress has been made on these fronts, Microsoft recognized that more must be done to limit the growing economic and political damage of state-sponsored attacks.[30]

The status of international agreement on the norms of cyberspace has worsened since Microsoft published the DGC. In July 2017, the GGE failed to reach consensus with reports indicating parties were split on whether to include language on the application of humanitarian law, the right of self-defense, and countermeasures.[31] Cuba and other parties resisted this language over concern about legitimizing the use of ICT for military action,[32] whereas the U.S. and allies supported the language to deter malicious activity and show the constraints of responses to malicious activities.[33]

Outside the GGE, Russia, China, and a number of central Asian governments have presented a different view of the future of cybersecurity and internet governance from those governments most supportive of the so-called internet freedom agenda. [34] The Shanghai Cooperative Organization (SCO) presented to the United Nations an International Code of Conduct for Information Security.[35] The proposed code puts more focus on the sovereignty of states in cyberspace, and to the extent it addresses human rights, it does so to explain how state limitations are consistent with human rights obligations.[36] Those governments have called for regulations regarding cybersecurity through engagement at the General Assembly, the International Telecommunications Union (ITU), and regional platforms.[37]

Despite the ideological and process differences, recent state action demonstrates the need for international agreement. A number of governments, including the U.S., Ukraine, Germany, and the U.K., based on a growing body of evidence, have accused Russia of interfering in elections.[38] Russian President Vladimir Putin has blamed U.S. development of hacking tools for undermining cybersecurity.[39] The accusations between Russia and the U.S. and European Union have increased public exposure to the scope and depth of harm of government hacking, but the implications go well beyond recent media coverage.

[27] http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174/.
[28] https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.
[29] http://www.g20.utoronto.ca/2015/151116-communique.html Para 26.
[30] http://www.g20.utoronto.ca/2015/151116-communique.html Para 26.
[31] Shttps://lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well.
[32] https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms.
[33] https://www.state.gov/s/cyberissues/releasesandremarks/272175.htm.
[34] For a list of Freedom Online Coalition Members visit https://freedomonlinecoalition.com/about-us/members.
[35] https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf.
[36] https://citizenlab.ca/2015/09/international-code-of-conduct.
[37] https://sputniknews.com/military/201708281056843131-russia-promote-cybersecurity-unga.
[38] http://www.newsweek.com/russia-election-hacking-france-us-606314; https://www.nytimes.com/2017/09/21/technology/facebook-russian-ads.html?mcubz=1&_r=0.
[39] https://www.washingtonpost.com/world/russias-putin-blames-us-cyberspies-for-developing-virus-used-in-global-hacking-wave/2017/05/15/a01602e0-3967-11e7-8854-21f359183e8c_story.html.

IV. A WORD ON THE GENEVA CONVENTION AND INTERNATIONAL NORMS

Solutions to these challenges clearly need to come from the international community at large rather than singular actors. While important groundwork for a multistakeholder approach is being laid down by the Freedom Online Coalition[40] and the UN GGE (whether a new one is established that reaches consensus or not), that approach should be rejuvenated with new emphasis on the harm that nation state attacks are causing for the users, including at-risk and vulnerable populations. The UN is uniquely placed in this regard, and we are hopeful that new initiatives such as the High Level Panel on Digital Cooperation[41] — which was launched by the UN Secretary General in July 2018 — will lead to more international commitments, and broader consensus on how to treat digital infrastructure with an eye on human rights and security, particularly around protecting the individual.

Existing practices have resulted in direct and indirect harms to users. Internet infrastructure is susceptible to attack, including against user-facing technology. North Korea accused the U.S. of sabotaging domestic connectivity, potentially in response to the breach of Sony Pictures.[42] The storage and weaponization of vulnerabilities also places users at risk outside government use. An exploit developed and held by the U.S. National Security Agency (NSA) called EternalBlue was leaked and was used in the WannaCry and NotPetya attacks, among others.[43] WannaCry alone will have reportedly caused an estimated $4 billion dollars in economic damage.[44] The attack implicated roughly 200,000 user devices and affected access to medical treatments.[45]

[40] https://freedomonlinecoalition.com/
[41] http://www.fao.org/e-agriculture/news/high-level-panel-digital-cooperation-launched-un-secretary-general
[42] https://www.cbsnews.com/news/north-korea-blames-u-s-for-internet-shutdown/
[43] https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html.
[44] https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses.
[45] http://www.abc.net.au/news/2017-05-15/ransomware-attack-to-hit-victims-in-australia-government-says/8526346; https://www.bbc.com/news/health-39899646/.

V. CONCLUSION

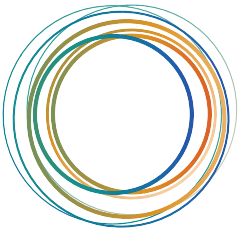
The companies that have committed to the Tech Accord — and Microsoft in initiating this discussion with its original Digital Geneva Convention proposal — have shown their understanding of the complexity of these issues and the nature of the threats that users face in their everyday interactions in the internet ecosystem. We welcome the opportunity to discuss what is needed to provide users with necessary protections, at a time when nation-state cybersecurity operations without strong international norms are threatening the health of our societies and the functioning of our democracies.

The Tech Accord can serve to pressure companies to act with integrity and stand as front-line defenders against the cyberattacks that harm users around the globe. As noted above, we believe the substance and process of the Tech Accord and DGC can be strengthened, but these initiatives show promise in encouraging companies and governments to take stronger measures to protect users against attack.

We encourage Microsoft to continue consultation on the methods by which mutually recognized attribution can function across multiple stakeholders, and to work with the companies that have pledged to the Tech Accord to continue developing those commitments. We also encourage all companies to adopt policies that promote user protections, and to vocally support human rights, digital security, and the rule of law.

Finally, we call for further engagement between civil society, governments, and public-sector stakeholders on the development of global norms to help protect users from cybersecurity threats, though established international fora and processes. Initiatives like the Tech Accord and the DGC are promising, but without grounding in globally recognized fundamental rights and support from diverse stakeholders, we may not see that promise fulfilled.

CONTACT



For more information, please visit our website **accessnow.org**, or contact:

Drew Mitnick | Policy Counsel | drew@accessnow.org

Lucie Krahulcova | EU Policy Analyst | lucie@accessnow.org