November 2017

accessnow.org

A POLICY MAKER'S GUIDE

TO THE GLOBAL CONFERENCE ON CYBERSPACE 2017

- Put users at the center of cybersecurity policy
- Apply systemic solutions to systemic problems such as digital security threats
- Use open and pluralistic processes to develop cybersecurity policy

Access Now defends and extends the digital rights of users at risk around the world. By combining innovative policy, global advocacy, and direct technical support, we fight for open and secure communications for all.

ACKNOWLEDGEMENTS

This paper is an Access Now publication. For any questions or suggestions, please contact Drew Mitnick, Lucie Krahulcova, and Raman Jit Singh Chima.

Special thanks to Sushovan Sircar, Amie Stepanovich, Peter Micek, and Maansi Verma, who also contributed to this report. We would also like to thank our staff for their input, in particular Donna Wentworth, Melody Patry, Brett Solomon, and the Policy Team for their review and oversight.

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

As chair of the first Global Conference on Cyberspace (GCCS) in London in 2011, UK Foreign Secretary William Hague proclaimed, "all human rights should carry full force online . . . Human rights are universal." However, the centrality of human rights to the conference has varied over the course of successive gatherings in Hungary, South Korea, and the Netherlands. Even when human rights are formally recognized at GCCS, and conference output statements achieve global recognition, there has been no satisfactory implementation of the commitments that are made. The 2017 GCCS, taking place in November in New Delhi, India, provides an opportunity to turn the tide and fulfill the promise implied in Hague's proclamation, making decisions that will strengthen cybersecurity while also safeguarding human rights.

This report provides delegates with the background, history, and context necessary for fruitful participation in the GCCS, including our recommendations for protecting human rights in cybersecurity policy. It urges the conference chair and delegations globally to take specific actions to implement these recommendations.

The theme of the GCCS has evolved over time. Each GCCS has covered, within the context of "cyberspace," social benefits, cybercrime, and international security; however, it was not until the most recent gathering in The Hague in the Netherlands in 2015 that organizers added "freedom and privacy" as a specific theme. It was also in 2015 that the chair's statement — the official output for most iterations of the GCCS — finally called for better protections for human rights.

The signature outcome of the Hague conference was the creation of the Global Forum on Cyber Expertise (GFCE), an institution that has promise for becoming an effective body for knowledge-sharing among stakeholders. However, for that promise to be realized, much more work is needed to increase access and participation by civil society organizations and technical security experts.

Further, even as conference outputs have included the language of human rights, the conference chairs have downplayed the centrality of these rights, and have in some cases invoked a false dichotomy between cybersecurity and protecting rights.

More troubling, however, is that the GCCS has yet to address international cybersecurity concerns from a user's perspective. This has led to oversight or neglect of critical issues in this area, including increasing violations of user privacy, state-conducted surveillance, attacks on strong encryption, government hacking, censorship, and state-ordered network disruptions.

Cybersecurity and human rights are mutually reinforcing objectives. However, governments have continued to emphasize increasing military and law enforcement control over digital networks, creating new risks for users and undermining the freedom, openness, and security of the internet. There is a significant danger of a global race to the bottom to secure such control, negatively impacting the digital security of all users and threatening the functioning of our networked systems and infrastructure. When states do not put human rights at the heart of cybersecurity policy, they put in jeopardy the capacity of the open internet as a global network for the realization of human rights across all nations.

In 2017, it is time to ensure that cybersecurity laws and practices protect the human rights of the people who use the internet. We urge the 2017 GCCS chair to adopt the recommendations below for the conference outputs, and the participating national delegations to commit to implementing these recommendations in policy.

RECOMMENDATIONS FOR THE GCCS CHAIR AND PARTICIPATING DELEGATIONS

To assist the chair and delegations in promoting and respecting human rights, Access Now has prepared a series of recommendations that we encourage the chair to adopt in conference statements, and the delegations to implement in policy. We urge participating governments at GCCS 2017 to:

- → **Put users at the center of cybersecurity policy**
- → **Apply systemic solutions to systemic problems such as digital security threats**
- → **Use open and pluralistic processes to develop cybersecurity policy**

Put users at the center of cybersecurity policy

User-centric cybersecurity policies protect users' rights. Policies that focus narrowly on state operations can undermine a government's international human rights obligations, threaten the peaceful use of the internet, inhibit access to information, and endanger the free flow of information. Governments must respect and protect the rights both to privacy and freedom of expression.

▶ RECOMMENDATION 1

Maintain human rights as the focus of conference statements and **avoid embracing the false dichotomy of "balancing" human rights and other interests** or **using sovereignty to justify** or **protect policies that fragment the internet.**

To demonstrate a commitment to human rights, conference statements should **draw from the language of human rights instruments**, including the Universal Declaration of Human Rights, International Covenant on Civil and Political Rights (ICCPR), and relevant UN resolutions, such as the Human Rights Council resolution on the promotion, protection, and enjoyment of human rights on the Internet, and standards like those developed by the Special Rapporteur on the freedom of expression on encryption, anonymity, and human rights.[1]

[1] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Human Rights Council, UN Doc.A/HRC/29/32 (May 22, 2015), available at http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/29/32; Resolution adopted by the Human Rights Council on the promotion, protection and enjoyment of human rights on the Internet, Human Rights Council, UN Doc.A/HRC/RES/32/13 (July 1, 2016), available at http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/32/13.

RECOMMENDATION 2

Acknowledge that, regardless of justification, **limits on the right to freedom of expression must be provided by law, address a legitimate aim, and be necessary to achieve that aim**, building on international standards in General Comment 34 on Article 19 of the ICCPR. Governments are increasingly censoring online content and restricting internet access. Intentional disruptions of internet access or other communications that render networks and services inaccessible for a specific population, or within a location, violate human rights, including freedom of expression. In addition, governments are exerting increased control over online content, such as by requiring platforms to remove certain categories of content. Such restrictions, often justified under the banner of combating extremism, harassment, hate speech, or "fake news," carry significant danger for interference with online expression.

RECOMMENDATION 3

Clearly **acknowledge the fundamental right to privacy and recognize necessary protections against overbroad surveillance authorities**, as articulated in the International Principles on the Application of Human Rights to Communications Surveillance.[2]

Apply systemic solutions to systemic problems such as digital security threats

Today's digital security threats are systemic problems that require systemic solutions. It is vitally important to protect our networks, data, and the end users who are the victims of a wide range of attacks. Holistic digital security approaches should address the risks of malware and vulnerabilities; social engineering attacks; restrictions on the functionality of a network; efforts to weaken the security and integrity of communications systems; and other threats to anonymity, privacy, and other human rights exercised online.

RECOMMENDATION 4

Address the human rights and cybersecurity implications of issues that GCCS has heretofore neglected, which have system-wide impacts: **state attacks on strong encryption, government hacking, vulnerable Internet of Things (IoT) networks, and flaws in the systems for cross-border access to data.**

Encryption and other digital security tools are necessary for ensuring the right to privacy and the exercise of freedom of opinion and expression in the digital age. It is critically important that the chair **acknowledge the necessity of strong encryption for ensuring the security of our communications and enabling the exercise of human rights online**.

Government hacking poses a great risk to human rights. These risks are compounded when hacking is conducted in the dark and without sufficient human rights protections for users. It is for this reason that **there should be presumptive prohibition on all government hacking, which can only be overcome in limited and exceptional circumstances (and only for information gathering purposes) when ten human rights safeguards are met.**[3] It is imperative that the chair **promote transparency into current hacking tools and authorities and initiate processes to ensure these tools are used in compliance with rights-respecting legal mechanisms.**

Internet of Things. There are insufficient safeguards, either in law or in practice, to address the impact of the Internet of Things on human rights. The increase in the number of connected devices, without adequate attention to security, not only threatens privacy but also enables significant systemic cybersecurity attacks.

[2] The International Principles on the Application of Human Rights to Communications Surveillance, https://en.necessaryandproportionate.org.
[3] Full text of the ten safeguards and Access Now's position on government hacking, *See* Amie Stepanovich, *A Human Rights Response to Government Hacking*, Access Now (Sep 2016), https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf.

The chair must **address the threat of insecure devices through protections to promote the security of data and ensure continued security updates**.

Cross-border data transfer. The systems for law enforcement access to data across borders in the context of criminal investigations is inefficient, and this has created incentives for policy that would harm human rights and limit the freedom and openness of the internet. It's urgent that the chair **promote means for lawful access across borders that improve efficiency for lawful government requests; reduce incentives for government interference with private sector platforms and networks; provide clarity for users, governments, and companies on the treatment of user data; and ensure the system for cross-border data requests protects users' rights**.

RECOMMENDATION 5

Address the threat of government hoarding and exploitation of vulnerabilities in software, devices, systems, and infrastructure. Hackers have used government-held digital security exploits and tactics for widescale attacks to gain access to personal and sensitive data, and these attacks have harmed human rights and caused widespread interruption of services. Governments undermine cybersecurity when they keep vulnerabilities secret and systematically prioritize offensive cyber operations and surveillance over cybersecurity defense. It is imperative that the chair **advance solutions to prevent damage to cybersecurity and human rights caused by states withholding information about critical vulnerabilities**.

Use open and pluralistic processes to develop cybersecurity policy

RECOMMENDATION 6

Ensure inclusivity and equal access for all stakeholders. At previous iterations of the GCCS, many substantive conversations took place in private rooms. Civil society has had limited or no involvement in these discussions, and there has been little transparency or public reporting on the proceedings. The chair should **foster an open and transparent decision-making process throughout the duration of the conference**, with clear lines of communication and feedback with all parties, including a mechanism for appeal and challenge. This would help to ensure that this conference, unlike its predecessors, is truly multi-stakeholder. To lead by example, the chair should further **commit to this level of open and pluralistic process domestically, in the Asia Pacific region, and internationally**. That means ensuring GCCS promotes inclusive and representative conversations. To achieve its goals, the Global Forum on Cyber Expertise (GFCE) must also become more inclusive, since civil society actors play a central role in ensuring rights-respecting cybersecurity.

RECOMMENDATION 7

Continue to pursue establishing necessary cybersecurity norms, as complementary to human rights law, including **limits on state actions that threaten the human rights and security of users.** Earlier this year, the UN Group of Governmental Experts failed to reach consensus on non-binding norms of state behavior, but the GCCS chair can continue that work.

The full text of the recommendations can be found on page 13 of this guide.

II. A PRIMER ON THE GCCS FOR NEW PARTICIPANTS

To participate effectively in the Global Conference on Cyberspace (GCCS), it's important to understand its purpose and history.

The GCCS is a multi-stakeholder platform for stakeholders around the world to develop consensus on norms for responsible behavior in cyberspace. First held in London in 2011, the conference has since been held in Budapest (2012), Seoul (2013), and most recently in The Hague in 2015. The GCCS convenes representatives from the governments of hundreds of countries, international organizations, civil society, academia, and the technical community. It works to "promote an open, free, and secure cyberspace" through discussions on practical cooperation in cyberspace, capacity building, commitments to respecting human rights online, and the practice of multi-stakeholderism.

GCCS aims to develop the voluntary and non-binding "rules of the road" for cyberspace.[4] Although not all conference goals have been met, attendance has been steadily rising since the inaugural conference in 2011.[5] The conference outputs typically gain global recognition yet the commitments made have yet to be implemented satisfactorily. For instance, even though the 2015 outcome document commits to a multi-stakeholder approach and respect for human rights online, there have since been increasing violations of user privacy, state-conducted surveillance, threats to strong encryption, internet shutdowns, muzzling of free expression online, and unauthorized government hacking. This is happening in regions around the world under the governance of GCCS-participating governments.[6]

The next gathering is in New Delhi, India on November 23 and 24, 2017, focusing on the theme, "Cyber4All: A Safe, Secure, and Inclusive Cyberspace for Sustainable Development." There are challenges ahead for organizers and participants alike. Organizers must ensure inclusivity and equal access for all stakeholders, while also ensuring that participants tackle issues in an open and transparent manner. Participants must respond to the pressing problems that this forum has overlooked, including attacks on strong encryption, vulnerable Internet of Things networks, problems with lawful cross-border access, and government hacking.

Below we present an analytical summary of the previous GCCS outputs with the aim of providing context for fruitful participation in the 2017 conference and guidance for leadership in addressing conference failures. We use the official chair statements as a primary source of information on the themes, consensus, and commitments that have been made at the GCCS, and address important developments such as the inclusion of new areas for norm development.

Review: thematic evolution of the GCCS

How has the focus of the GCCS evolved? Our analysis below traces the conference's themes, objectives, and language over time, including a review of the highlights and drawbacks for human rights and cybersecurity.

The GCCS was originally organized by the Foreign Office of the United Kingdom.[7] The UK created the first event to build on other fora that dealt with the internet and communications technology, including the two-phase World Summit on Information Society (WSIS).[8]

[4] *About* GCCS, GCCS 2017, https://gccs2017.in/about (last visited Oct. 23, 2017).
[5] *Id.*
[6] *Global Conference on Cyberspace 2015: Chair's Statement*, GCCS2015.com (Apr. 20, 2015), https://www.gov.uk/government/news/london-conference-on-cyberspace-chairs-statement. https://www.gccs2015.com/sites/default/files/documents/Chairs%20Statement%20GCCS2015%20-%2017%20April.pdf; *see also* https://www.accessnow.org/.
[7] *London: 1-2 November 2011*, GCCS 2015, https://www.gccs2015.com/london-1-2-november-2011 (last visited Oct. 23, 2017).
[8] *London Conference on Cyberspace: Chair's Statement*, GOV.UK (Nov. 2, 2011), https://www.gov.uk/government/news/london-conference-on-cyberspace-chairs-statement.

The WSIS gatherings were held in 2003 in Geneva, Switzerland and in 2005 in Tunis, Tunisia. The WSIS fora had aims similar to the GCCS and similarly fostered multi-stakeholder participation. However, a single government hosts each GCCS, while the WSIS process was overseen by the United Nations International Telecommunications Union (ITU), and it put more emphasis on development, specifically with the aim of promoting the use of Information and Communication Technology (ICTs) to achieve Development Goals.[9]

The host country for each GCCS develops the agenda and coordinates a chair's statement. Previous iterations of the GCCS have generated other outputs as well, including those developed during parallel and side-events.

LONDON, 2011

The UK government hosted the first GCCS, then called the London Conference on Cyberspace, on November 1-2, 2011.[10] As chair, UK Foreign Secretary William Hague said, ". . . it is my passionate conviction that all human rights should carry full force online: not just the right to privacy, but the right to freedom of expression. Human rights are universal."[11]

Two months prior to the London Conference, the Chinese and Russian delegations to the United Nations (UN) submitted to the General Assembly an "**International Code of Conduct for Information Security**" that put emphasis on sovereignty and territorial integrity.[12] The code also called for "curbing" the dissemination of certain information, including information that undermined a country's political environment, with caveat human rights language based on the premise of compliance with national laws. While the code called for a UN-hosted framework to reach consensus on the rules of cyberspace, the London Conference instead introduced principles and themes to serve as the basis for debate without the aim of establishing a formal or binding framework.

This first GCCS took place during a tumultuous period for the internet and communications technology. States were becoming more bold in conducting cyber attacks against other governments. They were also cracking down on dissent online. In late 2010, researchers discovered the Stuxnet worm that the U.S. and Israel used to conduct an attack on Iran's nuclear program.[13] It was also in 2010 that activists in the Arab world drew attention for using social media and communications technology in organizing the mass protests that swept the region.[14] While the significance of social media in the "Arab Spring" has been a source of debate, there is no question that a number of governments responded to the uprising with attempts to stop the coordination taking place on social media platforms.[15]

[9] *Why a Summit on the Information Society*, world summit on the information society, https://www.itu.int/net/wsis/basic/why.html (last visited Oct. 23, 2017).
[10] *Id.*
[11] Nick Hopkins, *Governments Must Not Censor Internet, Says William Hague*, The Guardian (Nov. 1, 2011), https://www.theguardian.com/technology/2011/nov/01/governments-must-not-censor-internet.
[12] UN General Assembly, Letter dated Sep. 12, 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, UN Doc. A/66/359 (Sep. 14, 2011), *available at* https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf.
[13] Robert McMillan, *New Spy Rootkit Targets Industrial Secrets*, Techworld (July 19, 2010), https://www.techworld.com/news/security/new-spy-rootkit-targets-industrial-secrets-3232365/.
[14] Ekaterina Stepanova, *The Role of Information Communication Technologies in the "Arab Spring,"* PONARS Eurasia Policy Memo (May 2011), http://pircenter.org/kosdata/page_doc/p2594_2.pdf; *see also #KeepItOn*, Access Now, https://www.accessnow.org/keepiton/ (last visited Oct. 23, 2017).
[15] *Id; see also* Jessi Hempel, *Social Media Made the Arab Spring, but Couldn't Save It*, Wired (Jan. 26, 2016), https://www.wired.com/2016/01/social-media-made-the-arab-spring-but-couldnt-save-it/.

The chair's statement from the London Conference focused on five themes:[16]

1. Economic growth and development
2. Social benefits
3. Safe and reliable access
4. International security
5. Cybercrime

Unfortunately, the agenda at the London conference failed to include some of the most pressing human rights challenges. For example, the themes and sub-themes do not mention the right to privacy, although there are references elsewhere to the "need to respect individual rights of privacy" as one of the principles for governing behavior in cyberspace that the chair announced earlier in 2011. Freedom of expression is also minimized, although it is mentioned as a sub-theme to "social benefits," and appears in notes by one participant in reference to concerns over censorship.

BUDAPEST, 2012

Hungary hosted the second GCCS in October 2012. Minister of Foreign Affairs, János Martonyi, chaired the conference with the goal of continuing the work of the London Conference.[17]

This conference was held three months after the UN Human Rights Council adopted a resolution on "[t]he Promotion, Protection, and Enjoyment of Human Rights on the Internet," which affirmed "the same rights that people have offline must also be protected online." Seventy countries, including Hungary and several other GCCS participants, had signed the resolution. This affirmation formed the basis for a better articulation of human rights in the subsequent gatherings of the GCCS.

The themes of the second iteration can be summarized using the subjects of the panel discussions:

1. Economic growth and development
2. Social benefits and human rights
3. Cybersecurity: building frameworks for prevention, response, and resilience
4. International security: state-on-state behavior and national security
5. Cybercrime

Importantly, this second conference introduces the promotion of cybersecurity and human rights.[18]

As the host, the Hungarian government emphasized international cooperation, including the participation of civil society, as necessary to preserve the internet as a platform for economic growth and communication. However, the UK government remained a steward of the conference, and in Budapest announced the creation and support for a global center on cybersecurity capacity-building that would work to improve coordination between and provide cybersecurity advice to countries.[19]

[16] *London Conference on Cyberspace: Chair's Statement*, GOV.UK (Nov. 2, 2011), https://www.gov.uk/government/news/london-conference-on-cyberspace-chairs-statement.
[17] *Summary by the Chairman János Martonyi, Minister of Foreign Affairs of Hungary*, https://www.gccs2015.com/sites/default/files/documents/Chair%27s%20Summary%20Budapest.pdf (last visited Oct. 23, 2017).
[18] *Id.*
[19] *Id.*

UK academic institutions have since adopted these goals, pursuing them in a body known as the Global Cyber Capacity Center (GCCC).[20]

The 2012 "Summary by the Chairman" tracked statements made by a number of governments and private-sector institutions, leading with a statement by the chair, and including a statement by a representative of China calling for balancing human rights and cybersecurity, and for establishing rules at the UN.[21] China's statement included five basic principles to guide the work of international cooperation, leading with sovereignty. The other four principles were (1) balance, (2) peaceful use of cyberspace, (3) equitable development, and (4) international cooperation, based on equality and mutual-benefit, increased mutual understanding, and trust.[22] The emphasis on sovereignty and balancing of human rights with other interests aligned with the Code of Conduct proposal previously submitted to the UN General Assembly.[23]

Unfortunately, the statement of the chair failed to acknowledge privacy as a fundamental human right, although it mentioned privacy in the context of data protection. Instead, the statement described privacy as "not only a technical concept but a political priority and also a business requirement." There is no mention of cybersecurity-motivated surveillance, either in the language of the output document or as a theme or topic at the conference. Moreover, there is no acknowledgement of the role governments play in undermining network security or the openness of the internet.

SEOUL, 2013

The Seoul Conference on Cyberspace was held in October, 2013. Organizers published the Seoul Framework for and Commitment to Open and Secure Cyberspace in preparation for the gathering. It was signed by 87 participant countries and has become one of the most important GCCS outcomes. The framework identified six "elements...for an open and secure cyberspace."[24] Those elements are:

1. Economic growth and development
2. Social and cultural benefits
3. Cybersecurity
4. International security
5. Cybercrime
6. Capacity building[25]

There was no separate statement from the chair, so the framework stands as the guiding document for the 2013 conference. The Seoul Framework is notable for its greater alignment of human rights language with that of the UN.[26] In addition to reiterating that the same rights that people have offline must also be protected online, the framework states that freedom of expression is applicable in accordance with Article 19 of the Universal Declaration

[20] *Global Cyber Security Capacity Centre: What are we doing?*, Oxford Martin School, http://www.oxfordmartin.ox.ac.uk/cybersecurity/ (last visited Oct. 23, 2017).

[21] *Global Conference on Cyberspace 2015: Chair's Statement*, Supra.

[22] *Id.*

[23] Letter dated Sep. 12, 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, *Supra*.

[24] *Seoul Framework for and Commitment to Open and Secure Cyberspace*, http://www.mofat.go.kr/english/visa/images/res/SeoulFramework.pdf (last visited Oct. 23, 2017).

[25] *Id.* The year prior to the Seoul event, the UN Group of Governmental Experts had issued a report that also highlighted capacity building. https://ccdcoe.org/sites/default/files/documents/UN-130624-GGEReport2013_0.pdf.

[26] *Id.*

of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR). While the framework indicates international law applies to cyberspace "regardless of frontiers and through any media of one's choice," it makes only a single mention of privacy and failed to identify it as a fundamental human right.

THE HAGUE, 2015

The last GCCS was held in The Hague, Netherlands, in April 2015. Ninety-nine countries participated and focused on efforts to "promote practical cooperation in cyberspace, to enhance cyber capacity building, and to discuss norms for responsible behavior in cyberspace."[27] The chair's statement called for a "forward-looking agenda to promote a free, open, and secure cyberspace."[28] Human rights, for the first time, were a focus of the chair's statement, marking significant progress.

In January 2015, prior to the GCCS, the UN General Assembly approved a resolution on "The Right to Privacy in the Digital Age" that calls for greater privacy protections online. Additionally, the same month as the GCCS, the UN's 2014-2015 Group of Governmental Experts on Cybersecurity convened for the third time to work on its report, which was published three months later.[29]

The chair's statement was broken down into eight themes. Five recalled themes from the earlier events:

1. Economic growth and social development
2. Cybersecurity
3. Cybercrime
4. International peace and security
5. Capacity building

However, there were three novel themes:

6. Freedom and privacy
7. Internet governance
8. Multi-stakeholder approach

Across several themes, the statement highlighted the need for better cooperation among stakeholders, in particular internationally to assist less-developed countries. Unfortunately, the 2015 GCCS itself failed to fully embrace this concept, providing only limited opportunities for collaboration with members of civil society and the technical community.[30]

[27] *About the Global Conference on Cyberspace*, Global Conference on Cyberspace 2015, https://www.gccs2015.com/gccs/all-about-gccs2015.
[28] *Global Conference on Cyberspace 2015: Chair's Statement, Supra*.
[29] Adam Segal, *The UN's Group of Governmental Experts on Cybersecurity*, Council on Foreign Relations (Apr. 13, 2015), https://www.cfr.org/blog/uns-group-governmental-experts-cybersecurity; *see also* UN General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/70/174 (July 22, 2015), http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174. The UN GGE report addressed norms of state behavior in cyberspace, including that "a State should not conduct or knowingly support ICT activity" that intentionally damages or critical infrastructure. The GCCS Chair's Statement did not call for such a limit on state conduct.
[30] Deniz Duru Aydin, *Global Conference on CyberSpace heavy on "cyber," light on solutions*, Access Now (Apr. 23, 2015), https://www.accessnow.org/global-conference-on-cyber-space-heavy-on-cyber-light-on-solutions/.

Additionally, the statement called for a "shared understanding" of how principles of state sovereignty and state activities apply online and identified security threats from state and non-state actors. For the first time in any iteration of GCCS, the statement recognized privacy as a human right and emphasized the need for citizens to have control of their data. Additionally, it called for a commitment to explore the development of "voluntary, non-legally-binding norms for responsible state behavior in cyberspace during peacetime."

Access Now's contribution and progress since 2015

Access Now participated in the 2015 GCCS and submitted comments for consideration for the chair's statement.[31] Based on a draft of the statement, we made a series of recommendations still relevant for the Delhi conference. Some of these suggestions, such as specifying that information sharing between the private sector and government must be narrow in scope, were reflected in the chair's statement from The Hague. Other recommendations, including those on the importance of refraining from undermining the security of communications technology and committing to the rights generally reflected in mutual legal assistance treaties, were not adopted.

We separated our recommendations for the draft chair's statement into provisions we supported, recommended additions, and changes to language. In the Appendix of this report, we summarize our recommendations.

Ultimately, the commitments made in the chair's statements at each GCCS are only as valuable as the participating governments' adherence to the commitments. The 2015 chair's statement noted the need to "improve the protection of the rights to privacy, freedom of expression and other relevant human rights, through appropriate national legislation, strong safeguards and effective oversight, consistent with international human rights law . . . we need to ensure that the collection and analysis of information by government institutions and private companies is not arbitrary or unlawful." The statement also promoted the joint "interest and responsibility" of government, businesses, and users in maintaining cybersecurity.

Despite recognizing the necessity of improving protections, many governments have since passed measures to further interfere with the human rights exercised online. For example, the UK government passed the Investigatory Powers Act, which provides legal cover for exhaustive UK surveillance programs.[32] Participating countries have also cracked down on essential digital security tools. China and Russia have enforced restrictions on the use of virtual private networks (VPNs) and the "Five Eyes" alliance has sought to limit the use of strong encryption.[33]

Global Forum of Cyber Experts (GFCE)

The Dutch government's signature outcome of the 2015 conference was the launch of the Global Forum on Cyber Expertise (GFCE), which remains active. The GFCE was

[31] *GCCS Chair Statement Feedback*, Access Now, https://www.accessnow.org/cms/assets/uploads/archive/GCCS%20Chair%20Statement%20Feedback%20Access.pdf (last visited Oct. 23, 2017).
[32] Drew Mitnick, *The UK Parliament shows disregard for digital rights by approving Snooper's Charter* (Nov. 17, 2016), https://www.accessnow.org/uk-parliament-shows-disregard-digital-rights-approving-snoopers-charter/
[33] Lily Hay Newman, *The Attack on Global Privacy Leaves Few Places to Turn*, Wired, (Aug. 4, 2017), https://www.wired.com/story/china-russia-vpn-crackdown/; Bill Gertz, *Deputy AG Calls for Court-Approved Access to Encrypted Devices*, The Washington Free Beacon (Oct. 11, 2017), http://freebeacon.com/national-security/deputy-ag-calls-court-approved-access-encrypted-devices/; Nick Everyshed, *Australia's Plan to Force Tech Giants to Give Up Encrpyted Messages May Not Add Up*, The Guardian (July 14, 2017), https://www.theguardian.com/technology/2017/jul/14/forcing-facebook-google-to-give-police-access-to-encrypted-messages-doesnt-add-up; https://techcrunch.com/2017/10/04/uk-gives-whatsapp-another-spanking-over-e2e-crypto/

established as a tangible implementation of the GCCS' key objectives: to promote practical cooperation in cyberspace, enhance cyber capacity building, and discuss norms for responsible behavior in cyberspace.[34]

In recognition of its embodiment of key themes from the 2015 conference, the GCFE was launched by 45 members, including a number of countries and companies like Microsoft, Huawei, and Vodafone.[35] The membership also comprises key international players such as the United States, India, Turkey, Germany, and Israel. However, other important governments are notably absent, including China and Russia, whose governments are involved in the Shanghai Cooperation Organization, which operates with a similar goal of providing a global cybersecurity platform. However, GFCE members are limited to governments, inter-governmental bodies, and private sector businesses. Civil society is permitted to participate as a partner, but as of publication, there were only six organizations listed as partners on the GFCE website.[36]

The forum held its first annual meeting in Brussels, Belgium on May 31, 2017, two weeks after the **WannaCry** ransomware attack spread rapidly among an estimated 300,000 computers across 150 countries. Exemplifying the contemporary challenges the GFCE faces, the WannaCry cryptoworm encrypted data and locked systems running outdated versions of Microsoft Windows, including computers in hospitals, schools, and gas companies. A Roadmap document published in 2017 states that the GFCE aims to organize high-level meetings on the margins of GCCS 2017 and all subsequent iterations.[37]

The GFCE has identified four areas to further its mission.[38] The first three are to serve as (1) "a knowledge repository and a place to exchange ideas on good practices," (2) "a coordination mechanism," and (3) a "clearinghouse that helps match members looking to share ideas and good practices." The last area is to, within its own functions, commit to an internet that is "free, open, and secure" and respect human rights, adhering to the UN Guiding Principles on Business and Human Rights and similar guidance.[39]

While the GFCE has yet to define its long term strategy, the institution has a unique opportunity to promote security solutions across governments and the private sector in ways that do not endanger human rights, but rather reinforce user protections. In order to better accomplish its goals, however, the GFCE must be a more inclusive institution for civil society actors who can play a central role in ensuring rights-respecting cybersecurity.

[34] The Hague Declaration on the GFCE defined it as a "pragmatic, action-oriented and flexible forum" that seeks to carry forward the "free, open and secure" agenda of the GCCS and act as a global platform for cyber capacity building and knowledge exchange. *Launch of the Global Forum on Cyber Expertise: The Hague Declaration on the GFCE* (Apr. 16, 2015), https://www.gccs2015.com/sites/default/files/documents/The%20Hague%20Declaration%20on%20the%20GFCE.pdf.
[35] *Id; see also Members of the Global Forum on Cyber Expertise*, Global Forum of Cyber Expertise (May 18, 2015), https://www.gccs2015.com/sites/default/files/documents/Members%20GFCE.pdf.
[36] *Overview Partners*, Global Forum of Cyber Expertise, https://www.thegfce.com/organization/partners/overview-partners, (last visited Oct. 30, 2017).
[37] *GFCE Roadmap 2017*, Global Conference on Cyber Expertise, https://www.thegfce.com/documents/publications/2017/02/15/gfce-roadmap-2017 (last visited Oct. 23, 2017).
[38] *Id.*
[39] *Id.*

III. THE 2017 GCCS IN NEW DELHI

AND ACCESS NOW'S RECOMMENDATIONS FOR THE CHAIR AND DELEGATES

India will host the fifth GCCS in New Delhi on November 23-24, 2017.[40] More than 2,000 delegates are expected to attend the conference, including representatives from over 100 countries. As of November 9, only 7 individuals of the 83 identified speakers were civil society (a mere 10%).[41] The chair for the conference is India's Union Minister for Electronics and Information Technology and Minister for Law, Mr. Ravi Shankar Prasad, and the vice-chair is Union Minister of State for Electronics and Information Technology, Culture, and Tourism, Mr. Alphons Kannanthanam.[42]

The goal of GCCS 2017 is to "promote an inclusive cyberspace" with focus on policies and frameworks for:

- Inclusivity
- Sustainability
- Development
- Security
- Safety and freedom,
- Technology and partnerships for upholding digital democracy
- Maximizing collaboration for strengthening security and safety
- Advocating dialogue for digital diplomacy[43]

In addition, the chair has identified four objectives:

- "to promote the importance of inclusiveness and human rights in global cyber policy,
- to defend the status quo of an open, interoperable and unregimented cyberspace,
- to create political commitment for capacity building initiatives to address the digital divide and assist countries, and
- to develop security solutions in a balanced fashion that duly acknowledge the importance of the private sector and technical community."

Finally, the chair has designated the main theme, "Cyber4All: A Safe, Secure, and Inclusive Cyberspace for Sustainable Development," which includes four sub-themes:

- Cyber4Growth
- Cyber4DigitalInclusion
- Cyber4Security
- Cyber4Diplomacy

While the chair has created a program that covers a wide range of topics, the lack of focus makes it difficult to discern what the chair seeks to achieve. The conference risks too broad a scope to ensure effective outcomes.

[40] *About GCCS*, GCCS 2017, https://gccs2017.in/about (last visited Oct. 23, 2017).
[41] Speakers: Civil Society, GCCS 2017, https://gccs2017.in/speakerscorner#civilsociety (last visited Oct. 23, 2017). Out of the identified civil society speakers, two are representatives of ICANN and one is currently serving as a chairman of national information technology agency.
[42] *Committee Members*, GCCS 2017, https://gccs2017.in/committee (last visited Oct. 30, 2017).
[43] *About GCCS*, GCCS 2017, https://gccs2017.in/about (last visited Oct. 30, 2017).

Recommendations for the chair and delegates

Since the 2015 GCCS, the situation for internet users has only gotten more dire, and today the security threats to the people who use the internet are pandemic. The 2017 chair must commit to strengthening cybersecurity, including specific protections for the rights of individuals. While previous conferences have promoted protections broadly, each time these commitments have failed to provide the substantive foundation for holding governments accountable. Yet human rights risks continue to increase, including those that are enabled under flawed cybersecurity laws and policies.

Laws and policies advanced under the banner of cybersecurity often interfere with human rights or undermine the security they seek to improve. Governments' continued emphasis on strengthening military and law enforcement control over digital networks has only increased risks for users and undermined the freedom and openness of the internet. Disclosure of secret government policies and operations and member behavior at international events indicate countries set policy for strategy and positioning rather than the security of the internet as a shared common resource. There is a significant danger of a global race to the bottom, negatively impacting the digital security of all users and posing a threat to the functioning of our global open internet.

Moreover, there are consistently more sophisticated security threats that interfere with the exercise of rights, from malware installed via phishing attacks and vulnerable Internet of Things devices conscripted into sophisticated botnets, to attacks that aim to damage public utilities or voting systems. In reality, threats may always persist. Ever-changing technology ensures the existence of vulnerabilities and further integration of the technology into our lives increases the impact of exploitation. The effects of poor digital insecurity includes — but also goes beyond — serious threats to users' privacy and expression, with particular threats to journalists, activists, and marginalized groups, and knock-on effects that endanger democratic processes and physical safety. Governments must be proactive and collaborative to prevent, reduce, and mitigate these threats.

To reverse these trends, we need a paradigm shift. Cybersecurity and human rights are mutually reinforcing objectives. The protection of human rights should be at the heart of cybersecurity policy development. Efforts on cybersecurity must be aimed at ensuring the functioning of the open internet as a global network that can help realize our human rights across all nations. We urge the participating governments at GCCS 2017 to:

→ **Put users at the center of cybersecurity policy**

→ **Apply systemic solutions to systemic problems such as digital security threats**

→ **Use open and pluralistic processes to develop cybersecurity policy**

Previous iterations of the GCCS have failed to address some of the most pressing security and human rights threats we face today. A user-centric approach to cybersecurity ensures measures to address these threats that conform to human rights obligations. Governments that justify overbroad surveillance programs or restrict access to the internet based on concerns about security fail to abide by commitments made at GCCS to promote an open and free internet. Moreover, the language of the previous gatherings has failed to promote security by defending essential digital security tools or addressing government actions that directly threaten the security and freedom of the internet. Finally, the process of establishing cybersecurity policy, both at the GCCS and elsewhere, has not been grounded in an appropriate process to enable effective participation across stakeholder groups, nor to ensure that the delegations that participate are held accountable for the commitments made.

We strongly urge the chair and conference delegates to heed these warnings and respond in line with our below recommendations. We believe these recommendations should be embraced in the final lead up to the conference to ensure that GCCS itself embodies the themes and principles it espouses.

Put users at the center of cybersecurity policy

RECOMMENDATION 1

Maintain human rights as the focus of conference statements and **avoid embracing the false dichotomy of "balancing" human rights and other interests** or **using sovereignty to justify or protect policies that fragment the internet**.

To demonstrate a commitment to human rights, conference statements should draw from the language of human rights instruments, including the Universal Declaration of Human Rights, International Covenant on Civil and Political Rights (ICCPR), and relevant UN resolutions, such as the Human Rights Council resolution on the promotion, protection, and enjoyment of human rights on the Internet, and standards like those developed by the Special Rapporteur on the freedom of expression on encryption, anonymity, and human rights.[44]

RECOMMENDATION 2

Acknowledge that, regardless of justification, **limits on the right to freedom of expression must be provided by law, address a legitimate aim, and be necessary to achieve that aim**, building on international standards in General Comment 34 on Article 19 of the ICCPR. Governments are increasingly censoring online content and restricting internet access. Intentional disruptions of internet access or other communications that render networks and services inaccessible for a specific population, or within a location, violate human rights, including freedom of expression. In addition, governments are exerting increased control over online content, such as by requiring platforms to remove certain categories of content. Such restrictions, often justified under the banner of combating extremism, harassment, hate speech, or "fake news," carry significant danger for interference with online expression.

RECOMMENDATION 3

Clearly **acknowledge the fundamental right to privacy** and **recognize necessary protections against overbroad surveillance authorities**, as articulated in the International Principles on the Application of Human Rights to Communications Surveillance.[45]

User-centric cybersecurity policies protect users' rights online. Policies that focus excessively on state operations undermine international human rights obligations, threaten the peaceful use of the internet, and inhibit the free flow of and access to information. Moreover, protections for the use of effective encryption and other digital security measures protect the rights to privacy and freedom of expression, among others. Secure and anonymous communications are essential to the exercise of human rights online.

Government hacking substantially interferes with human rights, including the right to privacy and freedom of expression.[46] While in many ways this interference may be similar to more traditional government activity, the nature of hacking creates new threats to human

[44] *Supra* note 1.
[45] The International Principles on the Application of Human Rights to Communications Surveillance, _*supra*.
[46] Stepanovich *supra* note 3.

rights that are greater in both scale and scope. Hacking can provide access to protected information, both stored or in transit, or even while it is being created or drafted. Exploits used in operations can act unpredictably, damaging hardware or software or infecting non-targets and compromising their information. Even when a particular hack is narrowly designed, it can have unexpected and unforeseen impact.

While not strictly a cybersecurity concern, the growing incidence of intentional disruptions of internet access by governments – termed "internet shutdowns"[47] – drew condemnation from the Human Rights Council.[48] Governments that restrict internet access commonly argue the shutdowns are necessary for national security or to ease public unrest.[49] Yet research shows internet shutdowns more often aim to suppress protest, and limit users' ability to access information essential for maintaining their own economic, social, and even physical security. Similarly, governments impose sweeping surveillance authorities and programs ostensibly to protect users. Human rights protections are essential for government efforts to maintain security, whether online or offline.

Apply systemic solutions to systemic problems such as digital security threats

RECOMMENDATION 4

Address the human rights and cybersecurity implications of issues that GCCS has heretofore neglected, which have system-wide impacts: **state attacks on strong encryption, government hacking, vulnerable IoT networks, and flaws in the systems for cross-border access to data**.

Encryption and other digital security tools are necessary for ensuring the right to privacy and the exercise of freedom of opinion and expression in the digital age. It is critically important that the chair **acknowledge the necessity of strong encryption for ensuring the security of our communications and enabling the exercise of human rights online**.

Government hacking poses a great risk to human rights. These risks are compounded when hacking is conducted in the dark and without sufficient human rights protections for users. It is for this reason that **there should be presumptive prohibition on all government hacking, which can only be overcome in limited and exceptional circumstances (and only for information gathering purposes) when the ten human rights safeguards are met.**[50] It is imperative that the chair **promote transparency into current hacking tools and authorities and initiate processes to ensure these tools are used in compliance with rights-respecting legal mechanisms**.

Internet of Things. There are insufficient safeguards, either in law or in practice, to address the impact of the Internet of Things on human rights. The increase in the number of connected devices, without adequate attention to security, not only threatens privacy but also enables significant systemic cybersecurity attacks. The chair must **address the threat of insecure devices through protections to promote the security of data and ensure continued security updates**.

Cross-border data transfer. The systems for law enforcement access to data across border in the context of criminal investigations is inefficient, and this has

[47] For a full list of internet shutdowns globally, see the Access Now "Shutdown Tracker Optimization Project (STOP)", at https://www.accessnow.org/keepiton-shutdown-tracker.
[48] A/HRC/RES/32/13 at para. 10 ("...condemns unequivocally measures to intentionally prevent or disrupt access...").
[49] Access Now "Shutdown Tracker Optimization Project (STOP), *Supra*.
[50] Full text of the ten safeguards and Access Now's position on government hacking, *See* Amie Stepanovich, *A Human Rights Response to Government Hacking*, Access Now (Sep 2016), https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf.

created incentives for policy that would harm human rights and limit the freedom and openness of the internet. It's urgent that the chair **promote means for lawful access across borders that improve efficiency for lawful government requests; reduce incentives for government interference with private sector platforms and networks; provide clarity for users, governments, and companies on the treatment of user data**; and e**nsure the system for cross-border data requests protects users' rights**.

RECOMMENDATION 5

Address the threat of government hoarding and exploitation of vulnerabilities in software, devices, systems, and infrastructure. Hackers have used government-held digital security exploits and tactics for widescale attacks to gain access to personal and sensitive data, and these attacks have harmed human rights and caused widespread interruption of services. Governments undermine cybersecurity when they keep vulnerabilities secret and systematically prioritize offensive cyber operations and surveillance over cybersecurity defense. It is imperative that the chair **advance solutions to prevent damage to cybersecurity and human rights caused by states withholding information about critical vulnerabilities**.

Today's digital security threats are systemic problems that require systemic solutions. It is vitally important to protect our networks, data, and the end users who are the victims of a wide range of attacks. Holistic digital security approaches should address the risks of malware and vulnerabilities; social engineering attacks; restrictions on the functionality of a network; efforts to weaken the security and integrity of communications systems; and other threats to anonymity, privacy, and other human rights exercised online.

States' duty to protect human rights includes the responsibility to proactively protect against third-party attacks, like those seen in large-scale ransomware and botnet attacks. However, states' duty to protect cannot itself justify violations of users' rights, such as unlawful restrictions on user anonymity protected by freedom of expression.

Use open and pluralistic processes to develop cybersecurity policy

RECOMMENDATION 6

Ensure inclusivity and equal access for all stakeholders. At previous iterations of the GCCS, many substantive conversations took place in private rooms. Civil society has had limited or no involvement in these discussions, and there has been little transparency or public reporting on the proceedings. The chair should **foster an open and transparent decision-making process throughout the duration of the conference**, with clear lines of communication and feedback with all parties, including a mechanism for appeal and challenge. This would help to ensure that this conference, unlike its predecessors, is truly multi-stakeholder. To lead by example, the chair should further **commit to this level of open and pluralistic process domestically, in the Asia Pacific region, and internationally**. That means ensuring GCCS promotes inclusive and representative conversations. To achieve its goals, the GFCE must also become more inclusive, since civil society actors play a central role in ensuring rights-respecting cybersecurity.

RECOMMENDATION 7

Continue to pursue establishing necessary cybersecurity norms, as complementary to human rights law, including **limits on state actions that threaten the human rights and security of users**. Earlier this year, the UN Group of Governmental Experts failed to reach consensus on non-binding norms of state behavior, but the GCCS chair can continue that work.

Fora where cybersecurity policies are formulated should respect institutionalized democratic processes. While the trend towards multi-stakeholderism has increased stakeholder representation, it has often failed to ensure meaningful participation.

Effective participation by all stakeholders entails equitable access to documents and decision-makers and designated opportunities for input in cybersecurity policy and norm establishment. This sort of open process should be supported by a pluralistic inclusion of stakeholders whereby various actors and groups are proactively approached for input and participation with a realistic timeframe that ensures space for appropriate consideration and opportunity for input. Multilateral government discussions often preference a single stakeholder group over the array of interests of those engaged on the future of the internet. Civil society actors should be invited to participate in the same depth as other stakeholders, and each session should be designed to provide a range of opinions and points of view.

IV. CONCLUSION

GCCS remains at the heart of the global conversation on cybersecurity and has demonstrated utility for creating lasting institutions to make progress on shared goals. Access Now encourages stakeholders from around the world to participate. We also urge the chair and delegations to integrate and affirm protections for human rights in their discussions and decision-making, and to embrace the principles of plurality and transparency in the process of developing outputs. We look forward to participating.

V. APPENDIX

ACCESS NOW'S FEEDBACK ON THE 2015 DRAFT CHAIR'S STATEMENT

Access Now participated in the 2015 GCCS and submitted comments for consideration for the chair's statement.[51] Based on a draft of the statement, we made a series of recommendations still relevant for the Delhi conference.

Provisions Access Now supported:

- Retaining all mentions of human rights
- Recognition of economic and security benefits of "privacy by design"
- Acknowledgement that human rights and security are complementary
- Recognition the right to privacy is integral to the realization of other human rights
- Welcoming of the newly established UN Special Rapporteur on the right to privacy

Recommendations for inclusion:

- Making clear the problem sought to be addressed by the GCCS and emphasize the need to transparently establish goals for cybersecurity, protect user's human rights, and avoid any overheated rhetoric ripe for abuse or fraught with vague and overbroad application
- Providing additional information on the GFCE and including adequate representation of civil society from all regions of the world
- Focusing on the role of governments in ensuring a free, open, and secure cyberspace
- Specifying that CSIRTs have a heightened responsibility to protect the privacy of the users dependent on their assistance
- Moving toward a user-centric approach to cybersecurity
- Including means of increasing mutual assistance in ways that protect the rights of individuals
- Referencing the International Principles on the Application of Human Rights to Communications Surveillance
- Clarifying that governments must not only assist in the development of norms of good behavior but act on those norms in good faith
- Including in the closing paragraph a reference to human rights

Recommended changes:

- Removing the overemphasis on state sovereignty that can be used to justify programs that fragment the internet
- Specifying that information shared between the private sector and government must be narrow enough in scope to protect the right to privacy of those whose information is shared
- Indicating crimes should not incur additional penalties merely because they were committed using a computer. Yet this continues to be the paradigmatic method for states to "update" their existing criminal laws for the digital realm.
- Indicating governments and corporations should use established mechanisms with recognized human rights protections for investigating crimes committed online rather than creating new or enhanced authorities that will have a disproportionate impact on online users.

[51] *GCCS Chair Statement Feedback*, Access Now, https://www.accessnow.org/cms/assets/uploads/archive/GCCS%20Chair%20Statement%20Feedback%20Access.pdf (last visited Oct. 23, 2017).

CONTACTS

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

Drew Mitnick | drew@accessnow.org

Lucie Krahulcova | lucie@accessnow.org

Raman Jit Singh Chima | raman@accessnow.org

accessnow

Access Now defends and extends the digital rights of users at risk around the world. By combining innovative policy, global advocacy, and direct technical support, we fight for open and secure communications for all.