GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

ADVANCING CYBERSTABILITY

FINAL REPORT

NOVEMBER 2019

GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

PROMOTING STABILITY IN CYBERSPACE TO BUILD PEACE AND PROSPERITY

The Global Commission on the Stability of Cyberspace (GCSC) will develop proposals for norms and policies to enhance international security and stability and guide responsible state and non-state behavior in cyberspace.

www.cyberstability.org
info@cyberstability.org | cyber@hcss.nl
@theGCSC

ADVANCING CYBERSTABILITY

FINAL REPORT

NOVEMBER 2019

***The Hague* Centre**
for Strategic Studies
Lange Voorhout 1
2514 EA The Hague

info@hcss.nl
www.hcss.nl

EastWest Institute
New York | Brussels
Moscow | San Francisco

cyber@eastwest.ngo
www.eastwest.ngo

CHAIRS

Michael Chertoff USA
Latha Reddy India
Marina Kaljurand Estonia *(former Chair)*

COMMISSIONERS

Abdul-Hakeem Ajijola Nigeria
Virgilio Almeida Brazil
Isaac Ben-Israel Israel
Scott Charney USA
Frédérick Douzet France
Anriette Esterhuysen South Africa
Jane Holl Lute USA
Nigel Inkster UK
Khoo Boon Hui Singapore
Wolfgang Kleinwächter Germany
Olaf Kolkman Netherlands
Lee Xiaodong China
James Lewis USA
Jeff Moss USA
Elina Noor Malaysia
Joseph S. Nye, Jr. USA
Christopher Painter USA
Uri Rosenthal Netherlands
Ilya Sachkov Russia
Samir Saran India
Marietje Schaake Netherlands
Motohiro Tsuchiya Japan
Bill Woodcock USA
Zhang Li China
Jonathan Zittrain USA

SPECIAL REPRESENTATIVES AND ADVISORS

Carl Bildt Sweden
Vint Cerf USA
Sorin Ducaru Romania
Martha Finnemore USA

DIRECTORS

Alexander Klimburg Austria
Bruce W. McConnell USA

RESEARCH ADVISORY GROUP CHAIRS

Sean Kanuck USA
Koichiro Komiyama Japan
Marília Maciel Brazil
Liis Vihul Estonia
Hugo Zylberberg France

SECRETARIAT

The Hague Centre for Strategic Studies

EastWest INSTITUTE

PARTNERS

Ministry of Foreign Affairs of the Netherlands

CSA SINGAPORE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

Internet Society

Microsoft

Afilias℠

SPONSORS

Federal Department of Foreign Affairs of Switzerland

GLOBSEC

Ministry of Foreign Affairs of Estonia

Ministry of Internal Affairs and Communications of Japan

SUPPORTERS

African Union Commission

Black Hat USA

DEF CON

European Union Delegation to the UN in Geneva

Global Forum on Cyber Expertise

Google

Municipality of The Hague

Packet Clearing House

Tel Aviv University

United Nations Institute for Disarmament Research

CONTENTS

LETTER FROM THE CHAIRS

Cyberspace represents one of the greatest inventions of mankind, reshaping personal, social, business, and political relationships. Unfortunately, due to attacks on and through cyberspace, urgent action is needed to ensure its stability. This concept of cyberspace stability—like its close cousin, international stability—requires a shared vision, one in which all parties recognize that geopolitical disagreements and changes which affect cyberspace must be managed in relative peace, and that cyberspace stability must be assured.

The Global Commission on the Stability of Cyberspace began its work convinced that an issue traditionally reserved to states—international peace and security—could no longer be addressed without engaging other stakeholders. Cyberspace is a multistakeholder environment: those who build and manage cyberspace, and those who respond to attacks on and through cyberspace, are as likely to be non-state actors as government officials. Our Commissioners were selected to reflect this characteristic. Besides former senior government officials with experience in international security issues, our ranks included acknowledged leaders from the fields of Internet governance, the human rights and development communities, and technology and industry. Together, our 28 Commissioners from 16 countries provided a wide range of experience and views, and they were aided by public comments in response to Commission outreach.

The Commission's final report represents three years of hard work. We gratefully recognize those who made this possible: our Commissioners, our advisors and researchers (many of them also volunteers), our financial supporters, and our management board. Finally, our appreciation goes to the Secretariat, which not only ably managed the process but was instrumental in the Commission's creation as a civil society initiative.

Throughout its work, the Commission remained cognizant of other cyberspace initiatives, both past and present. Our report—*Advancing Cyberstability*—complements and reinforces the work of others, while providing new ideas for advancing the stability of cyberspace.

Michael Chertoff
Co-Chair
Global Commission on the
Stability of Cyberspace

Reddy

Latha Reddy
Co-Chair
Global Commission on the
Stability of Cyberspace

EXECUTIVE SUMMARY

We have reached the end of a twenty-five-year period of strategic stability and relative peace among major powers. Conflict between states has taken new forms, and cyber activities are playing a leading role in this newly volatile environment. Over the last decade, the number and sophistication of cyber attacks by state and non-state actors have increased, thus threatening the stability of cyberspace. Simply put, people and organizations may no longer be confident in their ability to use cyberspace safely and securely, or be assured of the availability and integrity of services and information.

Against this backdrop, the Global Commission on the Stability of Cyberspace (GCSC) was convened to make recommendations for advancing cyberstability. We began by identifying a seven element Cyberstability Framework. This framework includes: (1) multistakeholder engagement; (2) cyberstability principles; (3) the development and implementation of voluntary norms; (4) adherence to international law; (5) confidence building measures; (6) capacity building; and (7) the open promulgation and widespread use of technical standards that ensure cyberspace is resilient. After defining this framework, the Commission explored in depth three of its elements: multistakeholder engagement, principles, and norms.

Multistakeholder engagement is called for in many international agreements, yet it remains contentious. Some continue to believe that ensuring international security and stability is almost exclusively the responsibility of states. In practice, however, the cyber battlefield (i.e., cyberspace) is designed, deployed, and operated primarily by non-state actors, and we believe their participation is necessary to ensure the stability of cyberspace. Moreover, their participation is inevitable, as non-state actors often are the first to respond to—and even to attribute—cyber attacks.

The Commission concluded that these non-state actors were not only critical for ensuring the stability of cyberspace, but that they too should be guided by principles and bound by norms. The four principles reflect this view, calling on all parties to be responsible, exercise restraint, take actions, and respect human rights:

- Responsibility: Everyone is responsible for ensuring the stability of cyberspace.
- Restraint: No state or non-state actor should take actions that impair the stability of cyberspace.
- Requirement to Act: State or non-state actors should take reasonable and appropriate steps to ensure the stability of cyberspace.
- Respect for Human Rights: Efforts to ensure the stability of cyberspace must respect human rights and the rule of law.

Building on these principles, and seeking to supplement and not duplicate the work of others, the Commission crafted eight norms designed to better ensure the stability of cyberspace and address technical concerns or gaps in previously declared norms:

1. State and non-state actors should neither conduct nor knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace.
2. State and non-state actors must not pursue, support or allow cyber operations intended to disrupt the technical infrastructure essential to elections, referenda or plebiscites.
3. State and non-state actors should not tamper with products and services in development and production, nor allow them to be tampered with, if doing so may substantially impair the stability of cyberspace.

4. State and non-state actors should not commandeer the general public’s ICT resources for use as botnets or for similar purposes.

5. States should create procedurally transparent frameworks to assess whether and when to disclose not publicly known vulnerabilities or flaws they are aware of in information systems and technologies. The default presumption should be in favor of disclosure.

6. Developers and producers of products and services on which the stability of cyberspace depends should (1) prioritize security and stability, (2) take reasonable steps to ensure that their products or services are free from significant vulnerabilities, and (3) take measures to timely mitigate vulnerabilities that are later discovered and to be transparent about their process. All actors have a duty to share information on vulnerabilities in order to help prevent or mitigate malicious cyber activity.

7. States should enact appropriate measures, including laws and regulations, to ensure basic cyber hygiene.

8. Non-state actors should not engage in offensive cyber operations and state actors should prevent such activities and respond if they occur.

Recommendations

Finally, recognizing both the importance of multistakeholder engagement and the fact that declaring behavior normative does not make it so, the Commission makes six recommendations which focus on strengthening the multistakeholder model, promoting norms adoption and implementation, and ensuring that those who violate norms are held accountable.

Specifically, the Commission recommends that:

1. State and non-state actors adopt and implement norms that increase the stability of cyberspace by promoting restraint and encouraging action.

2. State and non-state actors, consistent with their responsibilities and limitations, respond appropriately to norms violations, ensuring that those who violate norms face predictable and meaningful consequences.

3. State and non-state actors, including international institutions, increase efforts to train staff, build capacity and capabilities, promote a shared understanding of the importance of the stability of cyberspace, and take into account the disparate needs of different parties.

4. State and non-state actors collect, share, review, and publish information on norms violations and the impact of such activities.

5. State and non-state actors establish and support Communities of Interest to help ensure the stability of cyberspace.

6. A standing multistakeholder engagement mechanism be established to address stability issues, one where states, the private sector (including the technical community), and civil society are adequately involved and consulted.

The publication of this report represents both an end and a beginning. The Commission has fulfilled its mandate. For the members and supporters of the GCSC, however, as well as all those who support its goals, the hard work required to implement these principles, norms, and recommendations is just beginning. Begin it must, as the benefits of cyberspace will be lost if its stability is not ensured.

1. INTRODUCTION

The digital evolution and cyberspace have dramatically transformed human existence.[1] The ability to digitize, store, analyze, and transport data around the globe has had profound effects in every sector of society, and has changed the way we conduct personal, business, and political affairs. Today, approximately half the world's population is online[2] and this number is rapidly increasing. But even those not personally connected to cyberspace are affected by its reach, since the entities they rely upon to provide goods and services often use cyberspace for communications, logistics, and finance.

The benefits of cyberspace—and the need to ensure its stability—have often been discussed, as have its challenges. Most notably, cyberspace may support both noble and ignoble purposes. For example, global connectivity, anonymity, and lack of traceability permit individuals and machines to connect to data and systems without asserting identity, but criminals can also leverage these attributes to commit crimes with impunity. As a result, governments, companies, and people around the world are faced with conundrums. Governments are interested in protecting cyberspace, delivering public services, and promoting other important activities (e.g., education and online banking) but are also interested in advancing national security interests, including law enforcement, intelligence, and military capabilities. Companies, concerned about protecting their customers, reputations, and profits, find themselves under attack, investigating malicious activities, and/or subject to government data requests. People—whether they are themselves connected or not—are increasingly dependent on and embracing digital technology, but are concerned about its continued availability and integrity. Over the last decade, the number and sophistication of cyber attacks have increased, including attacks on government systems and critical infrastructures.[3] As such, neither the status quo nor the observable trends are encouraging.

Cyber attacks, which are conducted by both state and non-state actors, make clear that the world needs a Cyberstability Framework. Such a framework will serve to reduce the potential for significant disruptions of cyberspace that will undermine its benefits and reduce people's well-being, including their rights and freedoms. Clearly, well-designed and built products and services, managed well by IT professionals and computer users, will increase security and stability,

[1] "Cyberspace" has been defined in various ways. https://en.wikipedia.org/wiki/Cyberspace. The dictionary definition is "an electronic system that allows computer users around the world to communicate with each other or to access information for any purpose." https://dictionary.cambridge.org/us/dictionary/english/cyberspace. According to the United Kingdom, "Cyberspace is the term used to describe the electronic medium of digital networks used to store, modify and communicate information. It includes the Internet but also other information systems that support businesses, infrastructure and services." https://www.cpni.gov.uk/cyber. As such, it is arguably broader than the Internet, which is described in popular terms as a "global system of interconnected computer networks that use the Internet protocol suite (TCP/IP) to link devices worldwide." See https://en.wikipedia.org/wiki/Internet. See also International Telecommunication Union, "Defining the Internet," discussion paper (May 2013), https://www.itu.int/dms_pub/itu-s/md/13/wtpf13/inf/S13-WTPF13-INF-0008%21%21MSW-E.docx.

[2] "Internet Usage Statistics," Internet World Stats, last modified 4 October 2019, https://internetworldstats.com/stats.htm.

[3] Center for Strategic and International Studies (CSIS), *Significant Cyber Incidents Since 2006*, https://csis-prod.s3.amazonaws.com/s3fs-public/190904_Significant_Cyber_Events_List.pdf; Louis Marinos and Marco Lourenço, ed., *ENISA Threat Landscape Report 2018*, ENISA (January 2019), https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018; Abhishek Agrawal et al., *Microsoft Security Intelligence Report*, Vol. 24 (December 2018), https://clouddamcdnprodep.azureedge.net/gdc/gdc09FrGq/original; United Nations, General Assembly, *Developments in the field of information and telecommunications in the context of international security: report of the Secretary-General*, A/74/120 (24 June 2019), https://undocs.org/A/74/120.

just as poorly or negligently designed products and services, or poor or negligent operational practices, will undermine them. But better development and operations will not be enough, especially with state and non-state actors viewing cyberspace as a battlefield where one can achieve political, military, or economic advantage. A persistent attacker can defeat security measures, giving rise to the adage that "offense beats defense on the Internet" and creating instability.[4] Thus, it is important to focus not only on technology but on behaviors: how do we encourage all actors to behave in responsible ways that enhance—and do not threaten—the stability of cyberspace?

To help answer this question, several governmental and non-governmental entities supported the creation of the Global Commission on the Stability of Cyberspace (GCSC),[5] noting that:

> We have reached the end of a twenty-five-year period of strategic stability and relative peace among major powers. Conflict between states will take new forms, and cyber activities are likely to play a leading role in this newly volatile environment, thereby increasing the risk of undermining the peaceful use of cyberspace to facilitate the economic growth and the expansion of individual freedoms.
>
> In order to counter these developments, the Global Commission on the Stability of Cyberspace will develop proposals for norms and policies to enhance international security and stability and guide responsible state and non-state behavior in cyberspace. The GCSC will engage the full range of stakeholders to develop shared understandings, and its work will advance cyberstability by supporting information exchange and capacity building, basic research, and advocacy.[6]

Notably, the Commission itself is multistakeholder and global as it is comprised of individuals with diverse backgrounds and expertise. Some Commissioners have themselves served in government and were engaged in bilateral and multilateral negotiations on cyber issues, while others have experience in building, maintaining, and protecting the Internet itself. Others have represented civil society.

The Commission's work does not exist in a vacuum and the GCSC, recognizing that many other institutions and processes (both past and present) share its interest in the stability of cyberspace, has sought not to duplicate the work of others. Rather, the GCSC attempts to build upon other multistakeholder and governmental processes and influence future work. These processes include the foundational and ongoing work of the United Nations Group of Governmental Experts (UN GGE),[7] the work of the Open-Ended

[4] See, for example, P.W. Singer and Allan Friedman, "The Cult of the Cyber Offensive," *Foreign Policy* (15 January 2014), https://foreignpolicy.com/2014/01/15/cult-of-the-cyber-offensive/; World Economic Forum (WEF), *The Global Risks Report 2019*, (2019), http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf.

[5] For further information on the GCSC, see Appendix C: History, Goals, and Processes of the GCSC.

[6] Global Commission on the Stability of Cyberspace, https://cyberstability.org/.

[7] In an important resolution, in 2015 the United Nations General Assembly unanimously affirmed the conclusion of the UN GGE. See General Assembly resolution 70/237, *Resolution adopted by the General Assembly on 23 December 2015 [on the report of the First Committee (A/70/455)]*, https://undocs.org/en/A/RES/70/237. Thus, international law and, in particular, the Charter of the United Nations establish an exclusive framework for international response to hostile acts that also applies to cyber operations. Our work builds on the agreement by all states at the 2015 UN General Assembly to be guided by norms of responsible behavior to increase stability and security in the use of ICTs and to meet their commitments under international law for due diligence and cooperation.

Working Group (UN OEWG), as well as the efforts of the Global Forum on Cyber Expertise (GFCE),[8] World Summit on the Information Society (WSIS), the Global Commission on Internet Governance (the Bildt Commission), the Internet Governance Forum (IGF), the Global Conference on CyberSpace (GCCS/ the London Process), the NETmundial Initiative, the Organization for Security and Co-operation in Europe (OSCE), the African Union Commission (AUC), the Charter of Trust, the Cybersecurity Tech Accord, The Hague Program for Cyber Norms, the United Nations Institute for Disarmament Research (UNIDIR), the Paris Call for Trust and Security in Cyberspace ("the Paris Call"), and the UN Secretary-General's High-level Panel on Digital Cooperation. The Commission's work was also informed by commissioned research and requests for public comments.

Some of the efforts listed focused, in part, on cyberspace stability, and were concerned that cyberspace stability and governance are inextricably linked. That is, absent a robust governance model, society lacks the interactions and decision-making processes necessary to ensure stability. For example, the Bildt Commission proposed a multistakeholder social compact for the digital privacy and security "between citizens and their elected representatives, the judiciary, law enforcement and intelligence agencies, business, civil society and the internet technical community, with the goal of restoring trust and enhancing confidence in the internet."[9]

We commend these prior efforts at developing principles, rules, and norms to apply to behavior in the turbulent new domain of cyberspace and believe that a comprehensive framework is necessary to increase the stability of cyberspace. The historical record shows that societies and governments may in some cases take decades to develop broad, formal international governance structures for important new disruptive technologies.[10] The emergence of cyberspace as a crucial dimension of global economic, social, and security interdependence only dates from the late 1990s, when broad usage of the World Wide Web began. Thus, the evolving processes of governance are at an early stage where areas of normative coherence and incoherence co-exist.[11] For example, while norms and institutions related to the Domain Name System are well developed, there are major areas of disagreement among states and among companies related to content regulation. Sometimes, state and non-state actors apply norms from other regimes such as intellectual property and trade and, increasingly, private companies are themselves setting norms.[12] The purpose of our Commission is not to sort out these various questions of governance, but to put them within a general framework for ensuring the stability of cyberspace.

We also note that those concerned with the stability of cyberspace have struggled to keep up with those who seek to undermine it, as well as keep pace with technological developments and the evolution of geopolitical conflicts. Part of the challenge is that cyberspace has transformed the way actors pursue political and military objectives; with low barriers to entry, it is less difficult to become a cyber power than a traditional military power. Additionally, with new technology in their toolkits, some are hesitant to adopt constraints, particularly if those constraints are not widely honored. What is needed is an overarching Cyberstability Framework for the international community, one that promotes the stability of cyberspace yet remains useful as the pace of technological change continues to increase. We therefore start with defining the core objective: protecting the stability of cyberspace.

[8] The GFCE has been particularly active in capacity building. See, for example, "Delhi Communiqué on a GFCE Global Agenda for Cyber Capacity Building," Global Forum on Cyber Expertise (24 November 2017), https://www.thegfce.com/delhi-communique/documents/publications/2017/11/24/delhi-communique.

[9] Global Commission on Internet Governance, *One Internet* (2016), p. IX, https://www.cigionline.org/sites/default/files/gcig_final_report_-_with_cover.pdf. "We call on governments, private corporations, civil society, the technical community and individuals together to create a new social compact for the digital age."

[10] Perhaps the most pertinent example of a governance structure of this kind relates to nuclear weapons, which took significant time and effort to establish. Even now, 60 years on from the Treaty on the Non-Proliferation of Nuclear Weapons (NPT), the governance of nuclear weapons continues to be a security concern.

[11] This early stage has been called a "regime complex." See Joseph Nye, "The Regime Complex for Managing Complex Global Cyber Activities," Global Commission on Internet Governance, No. 1 (May 2014), https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf.

[12] See, for example, the norms developed by ISOC and Microsoft: "Mutually Agreed Norms for Routing Security (MANRS)," Internet Society (2014), https://www.manrs.org/; Angela McKay et al., *International Cybersecurity Norms Reducing Conflict in an Internet-dependent World*, Microsoft (December 2014), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVroA; and Scott Charney et al., *From Articulation to Implementation: Enabling Progress on Cybersecurity Norms*, Microsoft (June 2016), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmc8.

2. WHAT IS MEANT BY THE STABILITY OF CYBERSPACE?

DEFINITION:

Stability of cyberspace means everyone can be reasonably confident in their ability to use cyberspace safely and securely, where the availability and integrity of services and information provided in and through cyberspace are generally assured, where change is managed in relative peace, and where tensions are resolved in a non-escalatory manner.

While the Commission's definition builds on the standard definition of "stability,"[13] it is more nuanced in two ways. First, there is the reference to user confidence. Confidence is important because human decisions may be based upon perceptions, not just facts, and if someone perceives a lack of stability, they may be reluctant to use cyberspace and obtain its benefits. By way of example, the use of cyberspace may streamline processes and make them more efficient, thus suggesting that certain functions (e.g., access to government services, online banking) could benefit from leveraging cyberspace. But if such systems are unreliable—or there is a perception that such systems are unreliable—their use will be limited, and the benefits of the technology lost.

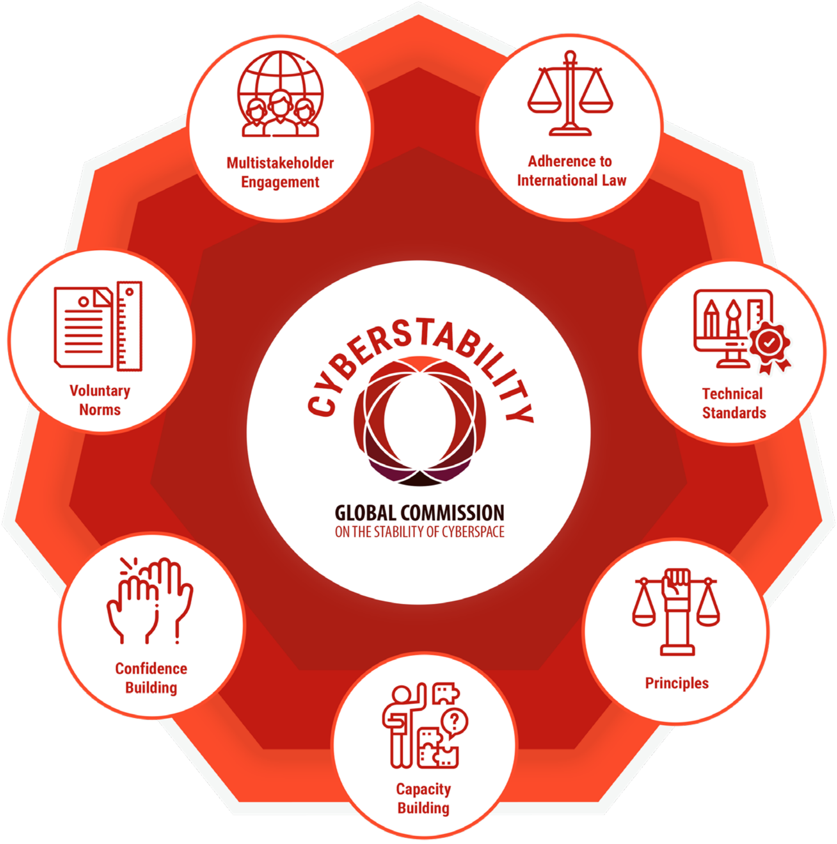
Second, it must be remembered that cyberspace is a domain of constant change. There are changes in technology, in business models, in functionality, and in societal expectations about the role of technology in daily life. Thus, unlike the dictionary definition of "stability" which includes "returning to an original condition," what we need are agile mechanisms to ensure the stability of cyberspace as technologies evolve. Simply put, everyone must remain confident in the availability and integrity of cyberspace even as it—and the world around it—changes.

[13] "Stability" is defined as "the state of being stable." https://www.lexico.com/en/definition/stability. Stable means (1) not likely to give way or overturn; firmly fixed; (2) not likely to change or fail; firmly established; and (3) not liable to undergo physical changes. See https://en.oxforddictionaries.com/definition/stable. In international relations, one of the most consistent definitions of the term international stability has been "the probability that the [international] system retains all of its essential characteristics; that no single nation becomes dominant; that most of its members continue to survive; and that large-scale war does not occur." Karl W. Deutsch and J. David Singer, "Multipolar Power Systems and International Stability," *World Politics*, Vol. 16, No. 3 (April 1964): 390-406, http://users.metu.edu.tr/utuba/Deutsch.pdf.

3. THE GCSC CYBERSTABILITY FRAMEWORK

To address the challenges described above, the GCSC, as others have done,[14] proposes a comprehensive Cyberstability Framework. This framework includes (1) multistakeholder engagement; (2) cyberstability principles; (3) the development and implementation of voluntary norms; (4) adherence to international law; (5) confidence building measures; (6) capacity building; and (7) the open promulgation and widespread use of technical standards that ensure cyberspace is resilient. The GCSC's efforts have focused primarily on three of these items—the multistakeholder approach, principles, and norms—and are addressed in Sections 4, 5, and 6, respectively. Regarding norms, we focused not just on their development, but on the more difficult issues of adoption, implementation, and accountability for violators.

We would note that there are many current efforts addressing individual elements of this Cyberstability Framework and these efforts are—like cyberspace itself—decentralized. To make progress, the GCSC believes that a concerted, global multistakeholder effort is required. Therefore, in addition to addressing substantive issues, the GCSC makes process recommendations that attempt to leverage and complement existing efforts and, perhaps, give them new energy.



[14] See, for example, *The Age of Digital Interdependence: Report of the UN Secretary-General's High-level Panel on Digital Cooperation* (June 2019), p.39, https://digitalcooperation.org/wp-content/uploads/2019/06/DigitalCooperation-report-web-FINAL-1.pdf. "We recommend the development of a Global Commitment on Digital Trust and Security to shape a shared vision, identify attributes of digital stability, elucidate and strengthen the implementation of norms for responsible uses of technology, and propose priorities for action."

The Cyberstability Framework image uses icons made by Freepik, monkik, smalllikeart, Eucalyp, Itim2101 from www.flaticon.com.

4. MULTISTAKEHOLDER ENGAGEMENT

Notwithstanding a plethora of international agreements among states citing the importance of a multistakeholder approach, it remains contentious. For some, the debate is philosophical and focuses on the comparative roles of state and non-state actors in technology policy and international affairs. For others, multistakeholder processes are practical, holding that states acting alone or with only minimal non-state input cannot ensure the stability of cyberspace.[15] We agree with this latter view.

This debate on the merits of multistakeholder engagement has gone on for decades. Often, the issue arose in the context of managing Internet resources, but the question of norms and national security were also raised. For example, during the second phase of the UN World Summit on the Information Society, the United Nations Working Group on Internet Governance (WGIG) rejected the concept of single stakeholder leadership. Rather, it concluded that the Internet is too large to be managed by one stakeholder group or one organization alone and proposed a multistakeholder approach. Thus, in 2005, the Heads of State in the WSIS Tunis Agenda declared that "A working definition of Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet."[16]

This view was reaffirmed ten years later by the High-Level Meeting of the UN General Assembly on the overall review of the implementation of the WSIS outcomes which also stated in UN resolution 70/125 (2015):

> We reaffirm, moreover, the value and principles of multi-stakeholder cooperation and engagement that have characterized the World Summit on the Information Society process since its inception, recognizing that effective participation, partnership and cooperation of Governments, the private sector, civil society, international organizations, the technical and academic communities and all other relevant stakeholders, within their respective roles and responsibilities, especially with balanced representation from developing countries, has been and continues to be vital in developing the information society.[17]

[15] "The WSIS definition (2005) introduced the concept of the 'respective roles' and the philosophy of 'sharing'. The NETmundial Declaration (2014) defined key elements as bottom up, openness, transparency, inclusiveness and human rights based. In other words, we have some general guidelines for a multistakeholder approach, but we do not have a single multistakeholder model. So far, two different multistakeholder models have emerged: the consultative model and the collaborative model." Wolfgang Kleinwächter, "Towards a Holistic Approach for Internet Related Public Policy Making," Global Commission on the Stability of Cyberspace (January 2018), https://cyberstability.org/wp-content/uploads/2018/02/GCSC_Kleinwachter-Thought-Piece-2018-1.pdf. For an additional discussion on multistakeholder models, see Virgilio Almeida et al., "The Origin and Evolution of Multistakeholder Models," *IEEE Internet Computing*, Vol. 19 (January-Feburary 2015): 74-79, https://doi.ieeecomputersociety.org/10.1109/MIC.2015.15.

[16] "Tunis Agenda for the Information Society," WSIS (18 November 2005), Paragraph 34, https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html.

[17] See United Nations General Assembly resolution 70/125, *Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society*, A/RES/70/125 (16 December 2015), Paragraph 3, https://undocs.org/en/A/RES/70/125.

Again, the statement went beyond the management of critical Internet resources and directly to the heart of national security issues:

> We recognize the leading role for Governments in cybersecurity matters relating to national security. We further recognize the important roles and contributions of all stakeholders, in their respective roles and responsibilities.[18]

Regarding norms specifically, the Group of Eight (G8) declared in 2011 that:

> The security of networks and services on the Internet is a multi-stakeholder issue. It requires coordination between governments, regional and international organizations, the private sector, [and] civil society...Governments have a role to play, informed by a full range of stakeholders, in helping to develop norms of behaviour and common approaches in the use of cyberspace.[19]

Two years later, in 2013, the UN GGE issued its *Report on Developments in the Field of Information and Telecommunications in the Context of International Security*. In a section entitled "Building cooperation for a peaceful, secure, resilient and open ICT environment," the UN GGE noted that "[w]hile States must lead in addressing these challenges, effective cooperation would benefit from the appropriate participation of the private sector and civil society."[20] The report went on to say, in a section entitled "Recommendations on norms, rules and principles of responsible behaviour by States," that:

> Member States should consider how best to cooperate in implementing the above norms and principles of responsible behaviour, including the role that may be played by private sector and civil society organizations.[21]

These positions were reaffirmed in the UN GGE's 2015 report, where it was declared that:

> While States have a primary responsibility for maintaining a secure and peaceful ICT environment, effective international cooperation would benefit from identifying mechanisms for the participation, as appropriate, of the private sector, academia and civil society organizations.[22]

This statement was repeated in a 2018 General Assembly resolution on *Advancing responsible State behaviour in cyberspace in the context of international security*.[23] Other international agreements clearly express the same sentiment; for example, the Paris Call stated, "We recognize the necessity of a strengthened multi-stakeholder approach and of additional efforts to reduce risks to the stability of cyberspace and to build-up confidence, capacity and trust."[24]

[18] Id., Paragraph 50.

[19] Group of Eight, "G8 Declaration: Renewed Commitment for Freedom and Democracy," G8 Deauville Summit (27 May 2011), Paragraph 17, http://www.g8.utoronto.ca/summit/2011deauville/2011-declaration-en.html.

[20] United Nations General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/68/98 (24 June 2013), p.7, Paragraph 12, https://undocs.org/A/68/98, (hereinafter, UN GGE 2013 Report).

[21] Id., p.8, Paragraph 25.

[22] United Nations General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174 (22 July 2015), p.13, Paragraph 31, https://undocs.org/A/70/174, (hereinafter, UN GGE 2015 Report).

[23] United Nations General Assembly resolution 73/266, *Advancing responsible State behaviour in cyberspace in the context of international security*, A/RES/73/266 (22 December 2018), https://undocs.org/en/A/RES/73/266.

[24] Ministry for Europe and Foreign Affairs of France, "Paris Call for Trust and Security in Cyberspace" (11 November 2018), https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf. See also, NETmundial, "NETmundial Multistakeholder Statement" (24 April 2014), http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf.

Most recently, in June 2019, the UN Secretary-General's High-level Panel on Digital Cooperation, in its report, *The Age of Digital Interdependence*, stated:

> Effective digital cooperation requires that multilateralism, despite current strains, be strengthened. It also requires that multilateralism be complemented by multi-stakeholderism—cooperation that involves not only governments but a far more diverse spectrum of other stakeholders such as civil society, academics, technologists and private sector.[25]

While the idea of a multistakeholder approach has proven to be successful, it is not universally supported. Some governments continue to believe that ensuring international security and stability is almost exclusively the responsibility of states. This more traditional view of security springs from the notion that states have the responsibility to protect their citizens from attack through forceful means, an idea reflected in the responsibilities of the United Nations Security Council as codified in Article 24 of the UN Charter.[26] This line of thinking may also be reinforced by past experience because, in the physical domain, governments not only enjoyed a monopoly over the legitimate use of force, but were also in control of the military grade weapons (e.g., airplanes, tanks) used to attack and defend that domain.

In practice, the cyber battlefield (i.e., cyberspace) is designed, deployed, and operated primarily by the private sector. Governments are, despite their unique responsibilities, not the exclusive protectors of this domain. Even if governments maintain a *de jure* monopoly over the legitimate use of force in cyberspace, they no longer have a practical monopoly on attacking and protecting this domain, nor can they prevent the proliferation and use of powerful cyber weapons. Rather, the technical community, civil society, and individuals also play a major role in the protection of cyberspace, including the promulgation of standards. Therefore, the multistakeholder approach is necessary to improve outcomes and ensure that the norms and policies supporting the stability of cyberspace are well-formed and avoid unwanted consequences.

Equally important, even if states wish to go it alone, they cannot. The participation of non-state actors in matters affecting the stability of cyberspace is unavoidable. For example, many members of the private sector and technical community may be responsible for critical protocols and services, and they may protect states that use their commercial and open source products. Additionally, even the investigation and attribution of attacks, a traditional role for and political prerogative of governments, is no longer their sole area of knowledge and responsibility; some notable state attacks have been identified and publicized by non-governmental entities. In short, even though states have a unique role to play during and after an attack (including law enforcement activity and/or taking diplomatic or other state actions), they have no monopoly on investigation and attribution, nor can they effectively exclude non-state actors. As a result, developing successful cyberspace norms and policies—and ensuring adherence to them—requires participation by, and is a responsibility of, all stakeholders, and governments must focus on creating mechanisms that effectively incorporate participation of the private sector, the technical community, academia, and other representatives of civil society. This is exactly what many governments have called for.

[25] *The Age of Digital Interdependence*, p. 7, https://digitalcooperation.org/wp-content/uploads/2019/06/DigitalCooperation-report-web-FINAL-1.pdf.

[26] Charter of the United Nations, "Chapter V – The Security Council," Repertory of Practice of United Nations Organs, http://legal.un.org/repertory/art24.shtml.

5. PRINCIPLES

Normative behavior derives from values. Declaring those values, whether they relate to individual responsibilities, state responsibilities, or fundamental human rights, must therefore be our starting point. Indeed, differing values can make achieving consensus difficult, as well as result in differing country or regional interpretations and implementations of international agreements. This is not to suggest that an agreement on principles is required for progress to be made; sometimes, parties agree on acceptable behaviors even if their motives for doing so differ. But shared principles and interdependence can lead to deeper commitments and reduce the risk of future disagreements or conflicts. It is therefore important that parties have candid discussions about the high-level principles which guide their thinking and from which norms flow.

The following four principles are critical to ensuring the stability of cyberspace:

1. **Responsibility:** Everyone is responsible for ensuring the stability of cyberspace.
2. **Restraint:** No state or non-state actor should take actions that impair the stability of cyberspace.
3. **Requirement to Act:** State or non-state actors should take reasonable and appropriate steps to ensure the stability of cyberspace.
4. **Respect for Human Rights:** Efforts to ensure the stability of cyberspace must respect human rights and the rule of law.

A. The Responsibility Principle

The first principle speaks to the decentralized and distributed nature of cyberspace. It reaffirms the need for a multistakeholder approach to ensuring the stability of cyberspace and, notably, extends "stakeholders" to include every individual. Every individual has responsibilities, in a personal and/or professional capacity, to ensure the stability of cyberspace. While it may be obvious that those responsible for government cyber policies and employees that manage cloud services have a role to play, every individual connected to cyberspace must take reasonable efforts to ensure their own devices are not compromised and, perhaps, used in attacks. Even those who are not connected to the Internet may be dependent upon its capabilities to receive goods and services, and they too have a stake in ensuring that cyberspace policy is being addressed appropriately in their communities.

B. The Restraint Principle

The second principle contains a general requirement of restraint. For states, this is consistent with the 2018 resolutions of the United Nations General Assembly (UNGA) concerning responsible state behavior in cyberspace[27] and the 2015 UN GGE report which notes that "Consistent with the purposes of the United Nations, including to maintain international peace and security, States should…prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security…"[28] But it is not just about states, as non-state actors can also engage in actions, such as hacking their attackers, that might also undermine the stability of cyberspace.

[27] United Nations General Assembly resolution 73/27, *Developments in the field of information and telecommunications in the context of international security*, A/RES/73/27 (5 December 2018), https://undocs.org/en/A/RES/73/27; and UN General Assembly resolution 73/266, https://undocs.org/en/A/RES/73/266.

[28] UN GGE Report 2015, p.7, Paragraph 13(a), https://undocs.org/A/70/174.

C. The Requirement to Act Principle

The third principle contains a general requirement to take affirmative action to preserve the stability of cyberspace. When acting, states should take care to avoid inadvertently escalating tensions or increasing instability. This is consistent with the obligation noted in the 2015 UN GGE report to "cooperate in developing and applying measures to increase stability and security in the use of ICTs."[29] But again, it is not just about states, as private companies and individuals can also take cooperative steps to help ensure the stability of cyberspace. For example, private companies can work together to mitigate cyber threats, and individuals can ensure they are employing best practices, such as upgrading, patching, and using multi-factor authentication, to reduce the risk that botnets will take over their machines and then be used to launch broad-based attacks that threaten the stability of cyberspace.

D. The Human Rights Principle

The fourth principle recognizes the importance of safeguarding human rights as an important element of cyberspace stability. As the reliance of individuals on information and communications technologies increases, the disruptive effect on human activity resulting from threats to its availability or integrity is amplified. Thus, it is imperative that as states pursue their national strategic interests in cyberspace, they give due consideration to the resulting impact on individuals, in particular their human rights. In a similar vein, non-state actors should consider and minimize risks that their activities pose to individuals' enjoyment of their rights online and offline. At a minimum, compliance with the Human Rights Principle requires that states abide by their human rights obligations under international law as they engage in activities in cyberspace.

Universally accepted human rights have been enshrined in the Universal Declaration of Human Rights.[30] Additionally, a large number of international agreements providing for a variety of specific human rights have been adopted and create binding legal obligations for state parties. In the context of cyberspace, the applicability of international human rights law has been explicitly confirmed on several occasions by the United Nations General Assembly,[31] the UN Human Rights Council (HRC),[32] as well as the UN GGE reports of 2013 and 2015.[33] Upholding rights and ensuring users trust that their rights are being respected is critical to ensuring the stability of cyberspace.

We note that the four principles are not intended to be all-inclusive or cover every aspect of cyberspace policy, and there are many organizations that have produced broad-based sets of principles covering a wide variety of issues. There are also other organizations focused on issues relating to Internet governance and human rights online (including privacy, freedom of expression, and freedom of association). Our goal is to achieve widespread acceptance of principles that support the stability of cyberspace, especially in an era of unprecedented and sophisticated hostile activity where rules may be unclear or, even if clear, may be neither embraced nor enforced.

[29] Id.

[30] United Nations General Assembly resolution 217 A (III), *Universal Declaration of Human Rights* (10 December 1948), https://www.un.org/en/universal-declaration-human-rights/.

[31] See United Nations General Assembly resolution 68/167, *The right to privacy in the digital age*, A/RES/68/167 (18 December 2013), https://undocs.org/A/RES/68/167; and United Nations General Assembly resolution 69/166, *The right to privacy in the digital age*, A/RES/69/166 (18 December 2014), https://undocs.org/A/RES/69/166.

[32] United Nations Human Rights Council, *The promotion, protection and enjoyment of human rights on the Internet*, A/HRC/20/L.13 (29 June 2012), https://undocs.org/A/HRC/20/L.13.

[33] UN GGE 2013 Report, https://undocs.org/A/68/98 and UN GGE 2015 Report, https://undocs.org/A/70/174.

6. NORMS

While principles are a key starting point for establishing policy and guiding tactical actions, their high level of abstraction requires that they be supplemented with more granular agreements that define acceptable behavior. This means that principles must be supplemented by norms. Norms represent social behaviors that are expected and appropriate.[34] It is impossible to discuss norms without referencing the work of other organizations, especially the UN GGE and its 2015 report.[35] The UN GGE recognized that "[g]iven the unique attributes of ICTs, additional norms could be developed over time,"[36] and the GCSC's mandate was, in fact, to "develop proposals for norms and policies to enhance international security and stability." To build on prior work and identify where additional norms may be warranted, it is important to start with the norms agreed to in 2015 which can be found, in their entirety, in Appendix A.

As the UN GGE noted in 2015, it was tasked to, among other things, "identify where additional norms that take into account the complexity and unique attributes of ICTs may need to be developed."[37] Since that time, ICT products and services—as well as their misuse—have continued to change. To address this, the GCSC focused on filling gaps in the current set of norms, adding technical specificity to the norms discussion, and addressing issues of implementation. Regarding filling gaps, for example, the GCSC endorsed a norm to protect the public core of the Internet[38] and a norm to protect electoral systems.[39] Similarly, while the UN GGE norm refers to the "integrity of the supply chain,"[40] a GCSC norm speaks more specifically to the types of supply chain attacks that must be addressed.[41]

The other major difference between the UN GGE norms and those proposed by the GCSC is that

[34] https://en.oxforddictionaries.com/definition/norm.

[35] UN GGE 2015 Report, https://undocs.org/A/70/174.

[36] Id., p.8, Paragraph 15.

[37] Id., p.7, Paragraph 11.

[38] Global Commission on the Stability of Cyberspace (GCSC), *Call to Protect the Public Core of the Internet* (New Delhi, November 2017), https://cyberstability.org/wp-content/uploads/2018/07/call-to-protect-the-public-core-of-the-internet.pdf. An early proponent of identifying the public core of the Internet for special protection was Dennis Broeders, a Dutch researcher. See Dennis Broeders, *The Public Core of the Internet: An International Agenda for Internet Governance* (Amsterdam: Amsterdam University Press, 2015), http://www.oapen.org/download?type=document&docid=610631.

[39] Global Commission on the Stability of Cyberspace (GCSC), *Call to Protect the Electoral Infrastructure* (Bratislava, May 2018), https://cyberstability.org/wp-content/uploads/2018/05/GCSC-Call-to-Protect-Electoral-Infrastructure.pdf.

[40] UN GGE Report 2015, p.8, Paragraph 13(i). "States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions."

[41] Global Commission on the Stability of Cyberspace (GCSC), *Norms Through Singapore* (November 2018), https://cyberstability.org/wp-content/uploads/2019/04/singaporenew-digital.pdf. "State and non-state actors should not tamper with products and services in development and production, nor allow them to be tampered with, if doing so may substantially impair the stability of cyberspace."

the GCSC believes that responsibilities should be imposed on non-state actors as well, as they must exercise restraint or take affirmative steps to ensure the stability of cyberspace. We are not referring here to cyber attacks by criminals; criminals who are not deterred by government action will not be deterred by norms. But since technology changes rapidly and laws do not, it is helpful to be precise about what non-state behaviors should be encouraged or discouraged even in the absence of laws. For example, some are advocating that victims of hacking should be allowed to "hack back." Even in the absence of laws permitting or prohibiting such conduct, the GCSC believes it inadvisable for several reasons, including the fact that the initial attacker may be routing its attack through third-party systems (e.g., a cloud provider or a hospital) and hacking back may therefore impact innocent users (e.g., cloud customers or patients). Additionally, due to these attacks on innocent victims, the hack back may be viewed as, or provoke, an escalation. In short, due to the complexities raised, even in the absence of laws, a norm restraining private sector actors may influence behavior and thus serve a salutary purpose.

A. The GCSC Proposed Norms

With the above points in mind, the GCSC developed the following proposed norms:

1. State and non-state actors should neither conduct nor knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace.

2. State and non-state actors must not pursue, support or allow cyber operations intended to disrupt the technical infrastructure essential to elections, referenda or plebiscites.

3. State and non-state actors should not tamper with products and services in development and production, nor allow them to be tampered with, if doing so may substantially impair the stability of cyberspace.

4. State and non-state actors should not commandeer the general public's ICT resources for use as botnets or for similar purposes.

5. States should create procedurally transparent frameworks to assess whether and when to disclose not publicly known vulnerabilities or flaws they are aware of in information systems and technologies. The default presumption should be in favor of disclosure.

6. Developers and producers of products and services on which the stability of cyberspace depends should (1) prioritize security and

stability, (2) take reasonable steps to ensure that their products or services are free from significant vulnerabilities, and (3) take measures to timely mitigate vulnerabilities that are later discovered and to be transparent about their process. All actors have a duty to share information on vulnerabilities in order to help prevent or mitigate malicious cyber activity.

7. States should enact appropriate measures, including laws and regulations, to ensure basic cyber hygiene.

8. Non-state actors should not engage in offensive cyber operations and state actors should prevent such activities and respond if they occur.

It is worth noting that finding the most appropriate language to express a norm can be challenging. If norms are too precise and leave no room for interpretation, it may be hard to achieve consensus and there may be significant gaps in coverage. On the other hand, if norms are too vague, they do not provide the type of guidance necessary to guide behavior and set clear expectations for a specific group of actors. The goal is to strike the right balance and develop further norms, where necessary, to ensure that unwanted behaviors are addressed. By way of example, the UN GGE norms adopted in 2015 protected critical infrastructures, but it is not clear that the public core of the Internet is covered by that term; many think of critical infrastructures as utilities and services (e.g., power, communications, and banking).[42] Additionally, the UN GGE did not specifically reference electoral systems, a concern that became more acute after 2015.[43] While electoral systems may be covered in some countries by reference (i.e., some states now consider electoral systems to be critical infrastructure, thus bringing them within the ambit of critical infrastructure norms),[44] certain countries may not follow this approach. Thus, while cyberspace is global, normative protections may not be. To help address interpretation issues regarding the GCSC norms, the Commission decided to provide background text for each norm described above (see Appendix B).

Finally, norms for behavior in cyberspace cannot be static. The GCSC norms reflect a moment in time in a continually changing technology landscape. State and non-state actors should be prepared to develop new norms as technologies advance, and as our understanding of the implications of existing technologies change.

Whether focused on UN GGE norms, GCSC norms, or other proposals, it must be recognized that for norms to be effective, it is necessary for them to be adopted and implemented, and norms violators must be held accountable. We now address those issues, before turning to how non-state actors, who are decentralized and distributed around the world, can come together to work with governments on practical solutions to cyberstability challenges.

B. Norms Adoption

For a norm to be effective, it must achieve widespread acceptance. Such acceptance, even by actors that some consider to be potential norm violators, bolsters the legitimacy of actions that call out norms violations and of appropriate collective actions taken to respond to such violations. While widespread

[42] Critical infrastructure has been defined as including “systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.” *Critical Infrastructures Protection Act of 2001*, 42 U.S. Code § 5195c(e), (2001). It has also been defined as “assets or systems which are vital for the maintenance of societal functions, health, safety, security, economic or social well-being of people.” Council of the European Union, *Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection*, Official Journal of the European Union, (8 December 2008), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114.

[43] Erik Brattberg and Tim Maurer, *Russian Election Interference: Europe’s Counter to Fake News and Cyber Attacks,* Carnegie Endowment for International Peace (23 May 2018), https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435. See also Michael McFaul, ed., *Securing American Elections*, Stanford Cyber Policy Center (June 2019), https://cyber.fsi.stanford.edu/securing-our-cyber-future.

[44] See, for example, U.S. Department of Homeland Security, “Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector” (6 January 2017), https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.

adoption is best, there is a place for smaller groupings of like-minded states or other entities to agree on and enforce particular norms. To address this, the GCSC is proposing a flexible, extensible approach that allows states and other stakeholders to embrace some norms while rejecting or abstaining from others. This approach not only creates clarity by highlighting specific areas of agreement and disagreement, but it permits particular norms to be embraced, refined, and implemented, even if more time is needed to evaluate others. In any case, widespread norms adoption will be a long-term effort.

There are also some unique and practical challenges to promoting norms adoption. The unique challenge is that we are attempting to address relatively new, destabilizing behaviors. To the extent a norm is "something that is usual, typical, or standard,"[45] drafting norms regarding future behavior is an interesting exercise. If everyone is already behaving a certain way, then a written norm is simply codifying existing practice. But if there is no "typical behavior," then drafting a norm is an attempt to encourage common behavior in the future, even where there is not common behavior today. Simply declaring something desirable will not make it normative, so adoption needs to be promoted.

Second, there needs to be greater awareness of proposed norms by the entities that are capable of their implementation, as well as those the norms are meant to protect. Even with significant activity in the UN and a host of other fora, norms adoption is still in its relative infancy and much needs to be done to promote proposed norms and secure acceptance, particularly in certain parts of the world. This is why capacity building efforts in this area are so vital; organizations with greater capacity are more likely to effectively support norms adoption and getting additional adherents is foundational to any global normative structure. Additionally, outreach must be done to those protected by norms, as they may be unaware of their potential impact. For example, there does not appear to be widespread awareness among Computer Emergency Response Teams (CSIRTs/CERTs) of the UN GGE norm concerning states not attacking national CSIRTs and using them for only defensive purposes. As discussed below, protected entities often will have a role in implementation and accountability (as well as the design of the proposed norm), but they cannot fulfill those roles if they have no awareness or insight into the proposals being made by state and non-state actors. It is clear that governments and international organizations need to do more to reach out to those communities that proposed norms are meant to help.

C. Norms Implementation

Following adoption, state and non-state actors must take concrete steps to implement a norm. There seems to be evolving consensus in the ongoing UN processes (OEWG and GGE) and in regional efforts that implementation is a priority.[46] To some, implementation refers to the adoption of the norm, engaging in capacity building efforts and confidence building measures, or reaching more granular consensus on the meaning of an agreed-to norm.[47] While these steps are important prerequisites to norms implementation, they do not serve to implement the norms themselves. For example, while capacity building is necessary to ensure that countries can secure themselves and have the bandwidth to engage internationally, one can build capacity without adopting or implementing norms. Similarly, while confidence building measures can help maintain the stability of cyberspace by facilitating the exchange of national views on cyber doctrine, establishing hotlines for rapid communications between national cyber experts, and encouraging the sharing of best practices and security standards, these too can be done

[45] See https://www.lexico.com/en/definition/norm.

[46] General Assembly resolution 73/266, p. 3, Paragraph 1(b), https://undocs.org/en/A/RES/73/266; General Assembly resolution 73/27, p. 5, Paragraph 5, https://undocs.org/en/A/RES/73/27. See also Organization for Security and Co-operation in Europe (OSCE), *Opening remarks by Secretary General Thomas Greminger*, 2019 Chairmanship OSCE-wide cyber/ICT security conference (Bratislava, 2019). "Regional organizations…can be incubators for new ideas and practical efforts that relate to CBMs as well as an implementer of globally accepted agreements, like the GGE reports. So, regional organizations are both incubators and implementers."

[47] The UN General Assembly invites all Member States, taking into account the assessments and recommendations contained in the reports of the GGE and the OEWG, to continue to inform the Secretary-General of their views and assessments on *inter alia* "Efforts taken at the national level to strengthen information security and promote international cooperation in this field" and "possible measures that could be taken by the international community to strengthen information security at the global level." See UN Secretary-General's report 74/120, https://undocs.org/A/74/120. For more national views of Member States, see, https://www.un.org/disarmament/ict-security/.

without implementing norms. Rather, implementing a norm involves taking concrete steps to give it force. Domestically, this might include incorporating proposed norms into national policy, legislation, and military doctrine. Internationally, this might include citing a norm's provisions when attributing attacks or taking diplomatic action. Operationalizing a norm in this way also serves to give it more precise definition.

D. Accountability

Once norms are adopted and implemented there must be accountability for those who violate them. This raises the complicated issues of attribution and response, both of which have proven challenging in addressing cyber attacks.

To support a claim that a state or non-state actor has acted wrongfully requires credible attribution. This starts with collecting and analyzing evidence, and there is both technical and procedural work that can be done now to improve the quality and timeliness of attribution. More specifically, as with other technical disciplines, having well-accepted protocols for collecting and analyzing evidence is important to improving the quality of investigations. Thus, the standardization of investigative methods is important because it may reduce concerns over the integrity of evidence, even if attribution must be decided on a case-by-case basis. In addition to improving attribution as a technical matter, there is much that can be done to shorten the bureaucratic processes associated with making attribution decisions and then, when appropriate, making them public. The often long delay between an event and a declaration of responsibility is due, in no small part, to unclear or unwieldy processes for reaching such decisions at a national level and is exacerbated when several countries are involved in making collective attribution statements. Designing and exercising processes for reaching attribution at a national level and international level, and improving information sharing between countries, can significantly improve the timeliness and effectiveness of attribution statements and facilitate any further appropriate action.

Even after the evidence points to a given actor, the next step (attribution) may remain challenging. In the past, some state and non-state actors have asserted that attribution is impossible or required absolute proof. But absolute proof is not required and while attribution may be difficult, it is not as insurmountable as some have suggested. In the nation state context, attribution, whether in the cyber or physical realm, is often a political act, and while there is no particular agreed upon standard of proof, countries still have a strong incentive to not make spurious allegations, lest they lose credibility. In short, what is needed is for attribution to be convincing to other countries and to the public.

Even if an aggrieved party is satisfied that a particular actor is responsible (and attribution has in fact occurred in international cases), holding actors truly accountable has also proven challenging, thus undermining the value of norms. After all, if there are no adverse consequences for those who violate accepted norms, those norms become little more than words on paper and they will be unlikely to discourage destabilizing activities.

Accountability for cyber attacks conducted by non-state actors is relatively straightforward and is predominately achieved through the imposition of civil or criminal responsibility under the domestic laws of the states concerned. There are certainly challenges in doing so, as the international nature of many cyber attacks and the technical challenges in collecting evidence may present obstacles to state action. But the way forward is conceptually clear: streamline international law enforcement processes and work to ensure that cyber criminals are identified and prosecuted.

Holding states accountable for norms violations is more challenging.[48] This is because responding to an attack in cyberspace is heavily context dependent. As to whether accountability is demanded, state and non-state actors will weigh different factors; for example, a state responding to a norms violation may consider the political implications while a private sector company may consider the business and reputational repercussions. As to how a norms violation should be addressed, state actions available in response to a norms violation can be viewed along a continuum, as a response may be minor (e.g., a private complaint), significant (e.g., economic sanctions), or dramatic (e.g., a highly visible kinetic response). While there is not and will not be a one size fits all response, clearly there must be meaningful consequences for violations of norms and international law. As past efforts to enforce norms have had limited success,

[48] States may be held responsible for the cyber operations they conduct, direct, or permit. The principle of due diligence may also prove helpful in defining the level of care required from states in cyberspace. Joanna Kulesza, *Due Diligence in International Law*, (Leiden: Brill Nijhoff, 2016), https://doi.org/10.1163/9789004325197. See also, *Articles on Responsibility of States for Internationally Wrongful Acts*, adopted by the International Law Commission at its fifty-third session in 2001, annexed to General Assembly resolution 56/83 of 12 December 2001, and corrected by document A/56/49(Vol I)/Corr4, Articles 4 and 11, http://legal.un.org/ilc/texts/instruments/draft_articles/9_6_2001.pdf.

more effective and timely responses are needed, recognizing that such responses should seek to minimize further instability.

Non-state actors are also working to ensure that norms violators are held accountable for their actions. For example, the GFCE[49] combines government, civil society, and private sector members to help coordinate efforts to build capacity, a necessary prerequisite to norms adoption, implementation, and accountability. Additionally, the private sector has taken on an expanded role in attributing attacks, using both proprietary and public information to expose actors and describe the damage they have caused. Finally, some private sector entities have proposed or launched efforts, such as the "CyberPeace Institute,"[50] that are designed to monitor and expose large cyber events in a more systematic way and potentially at greater scale.

Non-state actors should take a greater role in holding norms violators accountable for transgressions. The idea of private sector norms enforcement is not a new one: for instance, in 1977, during the anti-apartheid struggle in South Africa, General Motors promoted a set of widely-adopted principles for doing business (and not doing business) in that country, resulting in disinvestment by over 125 foreign businesses.[51] More recently, and in a more symbolic vein, many companies (and governments) responded to the Saudi murder of opposition reporter Jamal Khashoggi by boycotting the Future Investment Initiative as a message of disapproval.[52] These kinds of efforts bear further examination.

E. Communities of Interest

While a multistakeholder approach to norms adoption, implementation, and accountability is critical, harnessing the energies and capabilities of these groups is challenging. Governments often use the term "like-minded nations" to reflect a group of states with similar views, but there is no equivalent term that encompasses a collection of states, private companies, not-for-profit organizations (including standards organizations), civil society, and individuals that share views on a particular issue. This is important because the norms that have been proposed by the UN GGE and GCSC may affect different constituencies, and different organizations and members of society may be interested in advocating for certain norms more than others. Since governments, the private sector, the technical community, academia, and civil society are not monolithic entities, it is important to think about how to create a concerted as opposed to concentrated effort, one that engages diverse communities in norms-related issues.[53] Creating Communities of Interest permits those having expertise in specific norms to work on their further development and implementation. For example, Computer Emergency Response Teams (CERTs/ CSIRTs) may be particularly interested in implementing and monitoring the UN GGE norm aimed at protecting that community, just as those responsible for electoral systems may be particularly interested in the GCSC norm on electoral systems. Similarly, the Internet community could help advance, implement, and monitor the Commission's proposed norm on protecting the public core of the Internet, and developers may be most interested in the norm involving product tampering.

The formation of a Community of Interest may be directed or an ad hoc, bottom-up process. The fact that members themselves may form a Community does not suggest that their development and success should be left to chance. Instead, it is important to focus on what makes a Community successful: (1) shared principles; (2) issue focus; (3) subject matter expertise; (4) financial and administrative support; and (5) a transparent process. In fact, it may be possible to identify a best-practice template of how Communities should be created and implemented, thus allowing various norm-setting processes to leverage a similar Community model. This would help reconcile different workstreams to ensure efficiency and focus, as well as leverage best practices for norms adoption, implementation, and accountability.

[49] Global Forum on Cyber Expertise, https://www.thegfce.com/.

[50] CyberPeace Institute, https://cyberpeaceinstitute.org/.

[51] See, generally, "Sullivan Principles," Wikipedia, 12 August 2018, https://en.wikipedia.org/wiki/Sullivan_principles.

[52] See "Western boycott of Future Investment Initiative 2018," *Royal News*, 16 October 2018, https://en.royanews.tv/news/15500/2018-10-16.

[53] See, generally, *The Age of Digital Interdependence*, https://digitalcooperation.org/wp-content/uploads/2019/06/DigitalCo-operation-report-for-web.pdf.

7. RECOMMENDATIONS

Our six recommendations for ensuring the stability of cyberspace flow from our principles on responsibility, restraint, requirement to act, and respect for human rights. As everyone is responsible for, and a multistakeholder approach is critical to, ensuring the stability of cyberspace, our recommendations also seek to leverage the capabilities of state and non-state actors, in part through Communities of Interest. In short, we focus on what *should* be done and how it *might* be done.

1. **State and non-state actors must adopt and implement norms that increase the stability of cyberspace by promoting restraint and encouraging action.** State actors who have previously agreed to norms must more clearly define the terms used, an outcome that could be achieved through further negotiations and through practical experience implementing existing norms. Both state and non-state actors should offer clear evidence of norms adoption and implementation through public statements, and through changes in both policy and action.

2. **State and non-state actors, consistent with their responsibilities and limitations, must respond appropriately to norms violations, ensuring that those who violate norms face predictable and meaningful consequences.** Norms development and implementation will not be effective if those who violate norms learn that there is no price for doing so. Therefore, state and non-state actors should develop the internal capability to evaluate transgressions and quickly decide on and take appropriate individual and collective responses, consistent with the Requirement to Act Principle.

3. **State and non-state actors, including international institutions, should increase efforts to train staff, build capacity and capabilities, promote a shared understanding of the importance of the stability of cyberspace, and take into account the disparate needs of different parties.** Increasing capacity, capability, and understanding will broaden the world's ability to implement international laws, norms, and other confidence building measures designed to enhance the stability of cyberspace while respecting human rights. All parties should leverage existing organizations, including the multistakeholder Global Forum on Cyber Expertise, that are focused on capacity building as this is a prerequisite to adopting and implementing norms, ensuring accountability, taking other stability measures, and respecting human rights.

4. **State and non-state actors should collect, share, review, and publish information on norms violations and the impact of such activities.** While the world has seen actions that

would constitute a violation of the norms set forth in the United Nations and proposed by the GCSC, reporting tends to be anecdotal rather than comprehensive. Organizations, particularly those that are independent of any state or commercial interest, should systematically collect and publish information on norms violations and their impact. Doing so will serve to catalyze responses by state and non-state actors to norms violations and serve to improve norms compliance.

5. **State and non-state actors should establish and support Communities of Interest to help ensure the stability of cyberspace.** Establishing and supporting Communities will serve to ensure that all interested parties including states, the private sector, the technical community, academia, and civil society all fulfill their responsibility to ensure the stability of cyberspace. These Communities can focus on, among other things, the interpretation, adoption, and implementation of the cybersecurity norms put forward in this report and elsewhere, whether evidentiary standards for attribution are robust, and whether norms violators are being held accountable in a timely and effective manner.

6. **The GCSC recommends establishing a standing multistakeholder engagement mechanism to address stability issues, one where states, the private sector (including the technical community), and civil society are adequately involved and consulted.** The Responsibility Principle recognizes that everyone has a role to play in ensuring the stability of cyberspace and reinforces the need for multistakeholder approaches. From 2011-17, the Global Conference on CyberSpace (GCCS) provided one platform for such engagement that brought in minister-level participants from foreign and security ministries who were charged with achieving global stability in other contexts, and it was also the launching point of the Global Forum on Cyber Expertise, an important capacity building effort. The Internet Governance Forum (IGF) has also offered an important platform for multistakeholder discussion. More recently, the Paris Call brought together the largest-ever multistakeholder community of supporters of cybersecurity norms. These efforts suggest that the time is ripe for the development of a global, inclusive, and action-oriented multistakeholder community focused on the practical implementation of the cybersecurity norms put forward in this report and elsewhere. The mechanism should be supported by a standing structure to ensure a sustained and continuous effort.

APPENDIX A: NORMS ADOPTED BY THE UN GGE[54]

a. Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security;

b. In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences;

c. States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;

d. States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect;

e. States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression;

f. A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public;

g. States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions;

h. States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty;

i. States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions;

j. States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure;

k. States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.

[54] See United Nations General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174 (22 July 2015), https://undocs.org/A/70/174.

APPENDIX B: THE NORMS OF THE GCSC

1. NON-INTERFERENCE WITH THE PUBLIC CORE

NORM:

State and non-state actors should neither conduct nor knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace.

BACKGROUND

Defining the public core of the Internet is challenging as many different types of attacks may ultimately impair the general availability or integrity of the Internet writ-large (the outcome to be avoided). That said, there are clearly certain components that one would target if looking to have such a broad impact and it is at least possible to provide a non-exhaustive list of such critical elements. At the highest level, the Commission defines the phrase “general availability” to mean that the actor’s conduct has a substantial impact on the general population. Therefore, this norm recognizes that those states who support this norm may still engage in activities that are more limited in purpose and scope and have no substantial impact on the general population.

The Commission defines the phrase "the public core of the Internet" to include such critical elements of the infrastructure of the Internet as packet routing and forwarding, naming and numbering systems, the cryptographic mechanisms of security and identity, transmission media, software, and data centers.

Packet routing and forwarding elements include, but are not limited to, (1) the equipment, facilities, information, protocols, and systems that facilitate the transmission of packetized communications from their sources to their destinations; (2) Internet Exchange Points (the physical sites where Internet bandwidth is produced); (3) the peering and core routers of major networks which transport that bandwidth to users; (4) systems needed to assure routing authenticity and defend the network from abusive behavior; (5) the design, production, and supply-chain of equipment used for the above purposes; and (6) the integrity of the routing protocols themselves and their development, standardization, and maintenance processes.

Naming and numbering systems include, but are not limited to, (1) systems and information used in the operation of the Internet's Domain Name System (including registries, name servers, zone content, infrastructure and processes such as DNSSEC used to cryptographically sign records); (2) the WHOIS information services for the root zone, inverse-address hierarchy, country-code, geographic, and internationalized top-level domains and for new generic and non-military generic top-level domains; (3) frequently used public recursive DNS resolvers; (4) the systems of the Internet Assigned Numbers Authority and the Regional Internet Registries which make available and maintain the unique allocation of Internet Protocol addresses, Autonomous System Numbers, and Internet Protocol Identifiers; and (5) the naming and numbering protocols themselves and the integrity of the standardization processes and outcomes for protocol development and maintenance.

The cryptographic mechanisms of security and identity include, but are not limited to, (1) the cryptographic keys which are used to authenticate users and devices and secure Internet transactions; (2) the equipment, facilities, information, protocols, and systems that enable the production, communication, use, and deprecation of those keys; (3) PGP keyservers, Certificate Authorities and their Public Key Infrastructure; (4) DANE and its supporting protocols and infrastructure; (5) certificate revocation mechanisms and transparency logs; (6) password managers; (7) roaming access authenticators; (8) mechanisms of accurate time and establishment of temporal precedence, such as the Network Time Protocol and its infrastructure; (9) the integrity of the standardization processes and outcomes for cryptographic algorithm and protocol development and maintenance; and (10) the design, production, and supply-chain of equipment used to implement cryptographic processes.

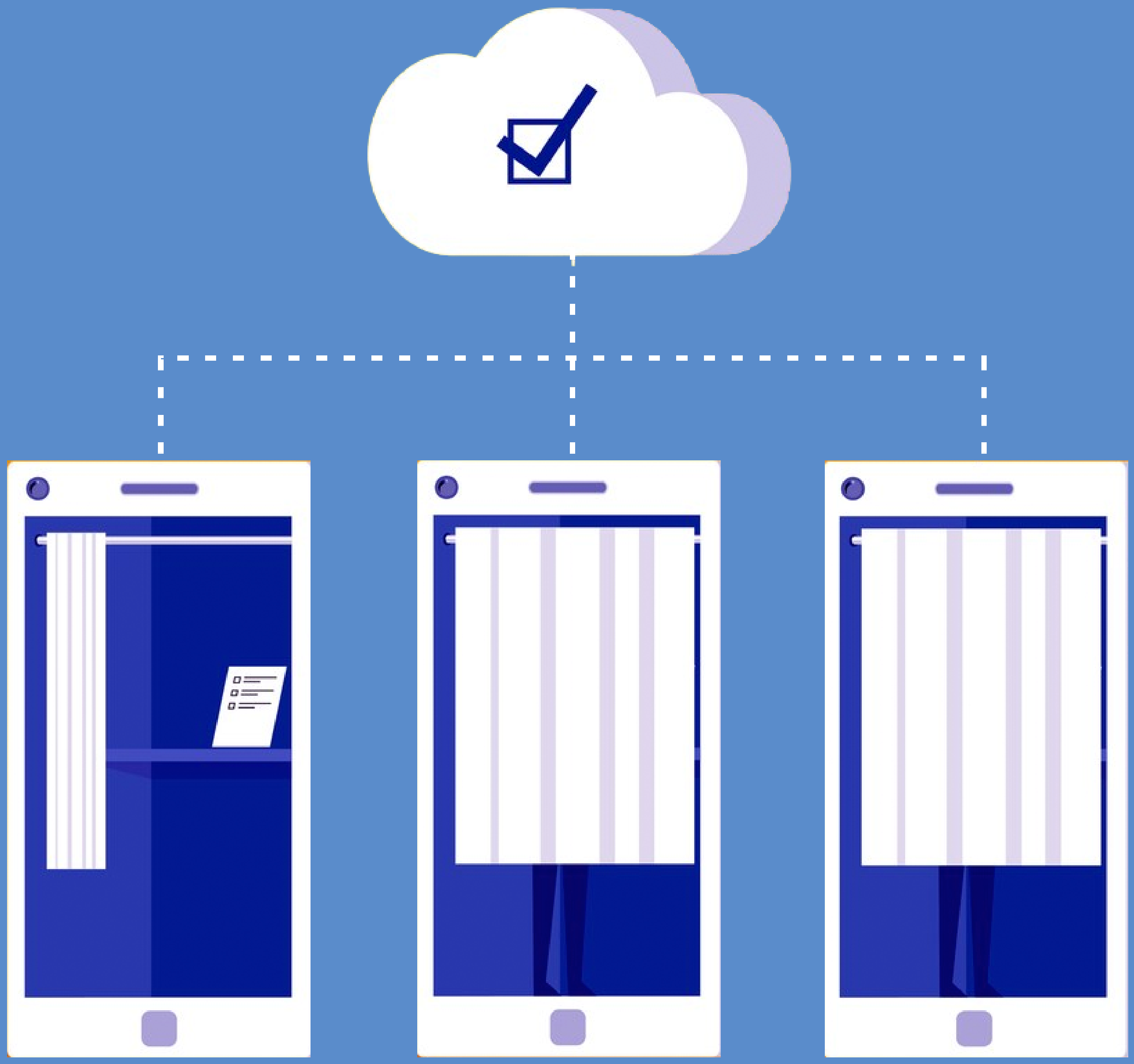
Transmission media includes, but are not limited to (1) infrastructure, systems and installations for communications serving the public, whether fiber, copper, or wireless; (2) terrestrial and undersea cables and the landing stations, datacenters, and other physical facilities which support them; (3) cellular and other wireless voice and data communications; (4) regulated and unregulated broadcast communications; (5) the support systems for transmission, signal regeneration, branching, multiplexing, and signal-to-noise discrimination; and (6) cable systems that serve regions or populations, but not those that serve the customers of individual companies.

Software includes but is not limited to the availability and integrity of the development processes, source code and patch-distribution infrastructure of software used in the core of the Internet and by large portions of the Internet-using public.

Datacenters include but are not limited to (1) the physical facilities which house servers, content, and Internet infrastructure; (2) the system used to ensure datacenter safety, security, physical access control, operations, management, maintenance, and redundancy systems; and (3) communications systems used to send communications to, from and within data centers.

Experts believe that far more categories of Internet and ICT-enabled infrastructure are deserving of protection, so this definition may be broadened in the future.

2. PROTECTING ELECTORAL INFRASTRUCTURE



NORM:

State and non-state actors must not pursue, support or allow cyber operations intended to disrupt the technical infrastructure essential to elections, referenda or plebiscites.

BACKGROUND

Of all the rules, precepts and principles that guide the conduct of states in the comity of nations, the norm of non-interference is perhaps held most sacred. Article 2(4) of the United Nations Charter articulates this norm and elevates it as a principle of legal, and thus, binding character:

> All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.

Through this provision, the framers of the Charter acknowledged that the gravest threats to the principle of non-intervention came from coercive measures directed at a state's physical or political autonomy, as, indeed, both are essential to state sovereignty. The territory controlled by a state may be a manifestation of its sovereign capacity, but it is worthless without the enjoyment of political agency and independence. Moreover, nothing reflects genuine political independence more than national participatory processes, such as elections, conducted freely and fairly. The UN Charter sought to grant strong protections against undue external interference. Those protective measures have now come to be challenged again in the digital age.

Experts have debated whether the type of cyber-related election interference recently seen amounts to an unlawful violation of sovereignty (because it interferes with the exercise of an inherently governmental function) or an unlawful intervention.[55] Whether or not a violation of international law has occurred, however, there is the clear possibility that malicious actors—acting alone, collectively, or on behalf of states—will manipulate elections through digital means. With national participatory processes becoming more complex in scale and sophistication, there has been a burgeoning of data, institutions and infrastructure to manage them. Many countries today publish their electoral rolls—a basic, traditional guarantee against voting manipulation or fraud—online, exposing such databases to cyber attacks and exploitation. Similarly, electoral voting instruments are used in far flung and remote areas of a country, where its operators are not fully abreast of the risks and concerns associated with their digital manipulation. Voting software suppliers and computer systems at the local or "booth" levels remain susceptible to such intrusions as well.

Seized of the growing number and intensity of threats to participative processes, and recognizing that such attacks are unacceptable, the GCSC recommends stronger national measures and effective international cooperation to prevent, mitigate and respond to cyber intrusions against the technical electoral infrastructure. The Commission acknowledges that the actual conduct of elections or participatory processes at the regional, local or federal level is firmly the remit of states, to be carried out in accordance with their respective national laws. Nevertheless, the cyber attacks on their electoral infrastructure may originate from outside the borders, necessitating multilateral cooperation resolution. As more countries opt to digitize their election machinery, the risks and vulnerabilities associated with such infrastructure increase manifold, as does the prospect of a major, offensive cyber operation. Thus, governments must commit to refraining from engaging in cyber operations against the technical electoral infrastructure of another state. In recommending this norm, the Commission merely affirms that election interference is intolerable whether it is considered to be a violation of international law or not.

[55] See Michael N. Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law," *Chicago Journal of International Law*, Vol. 19, No. 1, and Nicholas Tsagourias, "Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace," https://www.ejiltalk.org/electoral-cyber-interference-self-determination-and-the-principle-of-non-intervention-in-cyberspace/.

3. NORM TO AVOID TAMPERING

NORM:

State and non-state actors should not tamper with products and services in development and production, nor allow them to be tampered with, if doing so may substantially impair the stability of cyberspace.

BACKGROUND

In a norm focused on "Non-Interference with the public core of the Internet," the GCSC called upon state and non-state actors not to intentionally and substantially damage the general availability or integrity of the public core of the Internet. In support of this norm, the Commission noted the increasing dependence of other infrastructures on a stable and secure Internet and the potential dramatic consequences of its disruption. While the public core norm focused on the "core of the Internet," individuals and organizations rely heavily upon certain commercial products to reach that public core and leverage the connectivity it provides. As a result, tampering with key components in software and hardware IT products (including, but not limited to, operating systems, Industrial Control Systems, switches, routers and other critical networking equipment, critical cryptographic products and standards, microchip design and widely used end-user consumer applications) may similarly deprive society of the ability to use and leverage the Internet safely and securely, and weaken overall the trust in its proper function. While such attacks are often in the news, what receives less attention is the fact that an attack can occur even before a product or its update reaches the market. For example, a product can be attacked by inserting a vulnerability—or secretly removing a security feature—during the design and manufacturing phase or during one of its updates. Put another way, a product can be tampered with prior to its release or production, with consequences for the public at large. The time between inserting a vulnerability, and activating the vulnerability for malicious use, can vary.

States have conflicting interests and responsibilities when dealing with information technology products. On the one hand, they have an obligation to promote the resilience and integrity of the cyber infrastructure to help thwart future cyber attacks by malicious actors and make the entire digital ecosystem safer. On the other hand, states have an obligation to their citizens to protect national security and combat criminals and other malicious actors in cyberspace. The exploitation of vulnerabilities in digital products and services used by adversaries has been leveraged by states to achieve their national security and public safety mission. Thus, to the extent that states consider exploiting vulnerabilities to be an effective approach to fulfilling their responsibilities, they may also find it helpful to intentionally introduce weaknesses or back doors into products and services used by adversaries. Non-state actors may in turn tamper with products and services as well, as their objectives may be aided by their ability to disrupt the stability of cyberspace. It is important to note that the norm prohibits tampering with a product or service line, which puts the stability of cyberspace at risk. This norm would not prohibit targeted state action that poses little risk to the overall stability of cyberspace; for example, the targeted interception and tampering of a limited number of end-user devices in order to facilitate military espionage or criminal investigations. This type of activity, unless it occurs within the basic infrastructure of the public core itself, or critically weakens user trust in the Internet globally, is unlikely to weaken the overall trust in cyberspace that is a condition of cyberstability. Although a non-state actor may also target systems in a limited way, such activity might violate existing criminal and civil laws.

While state and non-state actors should not affirmatively tamper with products in development or production, those in industry also have a responsibility to prevent such activities. Therefore, those creating products and services must commit to a reasonable level of diligence in the designing, developing and delivering of products and services that prioritizes security and in turn reduces the likelihood, frequency, exploitability and severity of vulnerabilities. Those concerned must also reject any apparent state or non-state efforts to compromise products and services, as well as adopt practices that reduce the risk of tampering and permit them to respond if tampering is discovered.

4. NORM AGAINST COMMANDEERING OF ICT DEVICES INTO BOTNETS

NORM:

State and non-state actors should not commandeer the general public's ICT resources for use as botnets or for similar purposes.

BACKGROUND

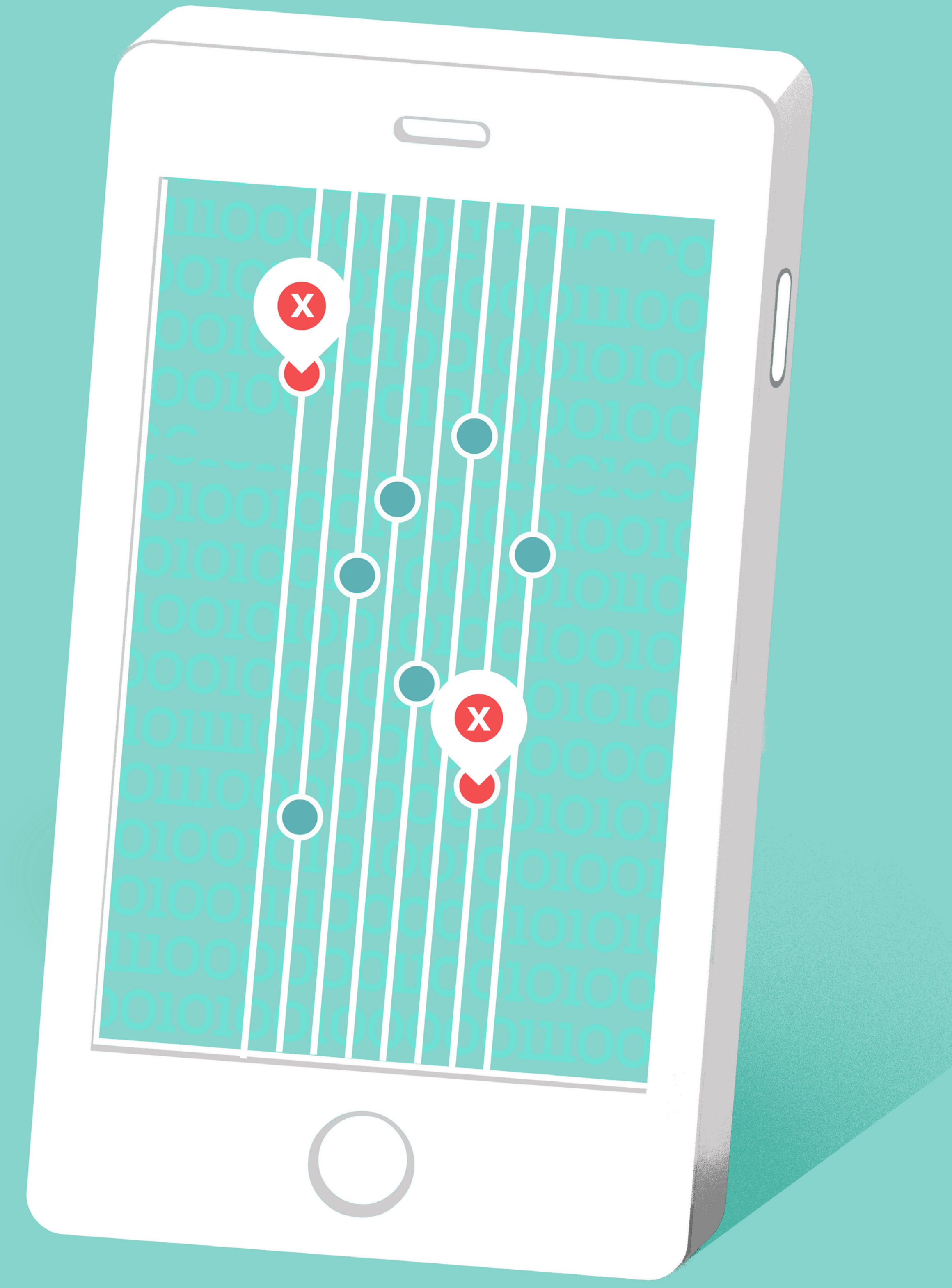
Internet-connected devices are becoming integral to people's lives globally. We are surrounded by devices with a multiplicity of computational, networking, sensing and actuating capabilities. Thermostats, televisions, medical devices, alarm clocks and automobiles have computing, storage and network capacity that can be appropriated and abused. Exploits of vulnerabilities in their underlying code can lead to physical safety issues for the individuals using the device: a device working outside of its design parameters could catch fire or create other unsafe conditions, such as unexpectedly unlocked doors, video broadcast from the interior of a house or cause (medical) equipment to fail.

We refer to botnets when software agents are installed, en masse and without consent, to use the devices' computational, storage or network resources. Those botnets can then be used to exercise direct effects on a different targeted system that can include impacting the end-targets' data confidentiality, availability and integrity. Therefore, a potentially uninvolved "third party" device, and its owner/operator, are made party to a malicious cyber activity without their knowledge. The compromise of devices to install malicious software agents not only weakens the defense of the device from other attacks—for instance from criminals—or infringes on the devices' normal functioning, but also casts the owner/operator as potentially culpable for damages inflicted on the end target. This is particularly acute for cases where the compromise of the device might inadvertently cast the device and its owner/operator as an unwitting belligerent in interstate hostilities, and therefore invite reprisals or liability.

As we become increasingly reliant on technology in our personal environment, and more and more connected devices enter the market, the exploitation of consumer devices and their use as botnets increasingly undermines trust and destabilizes society. The Commission recognizes that there are cases—for instance for law enforcement purposes—in which authorized state actors may find it necessary to install software agents on devices of a specifically targeted individual adversary, or a group of adversaries. However, state and non-state actors should not commandeer civilian devices of the general public (en masse) to facilitate or directly execute offensive cyber operations, irrespective of motivation.[56]

[56] This norm is complementary to the previous proposed norm for state and non-state actors to avoid tampering with products prior to their release, which focuses on supply chain aspects, while this norm addresses already deployed devices.

5. NORM FOR STATES TO CREATE A VULNERABILITY EQUITIES PROCESS



NORM:

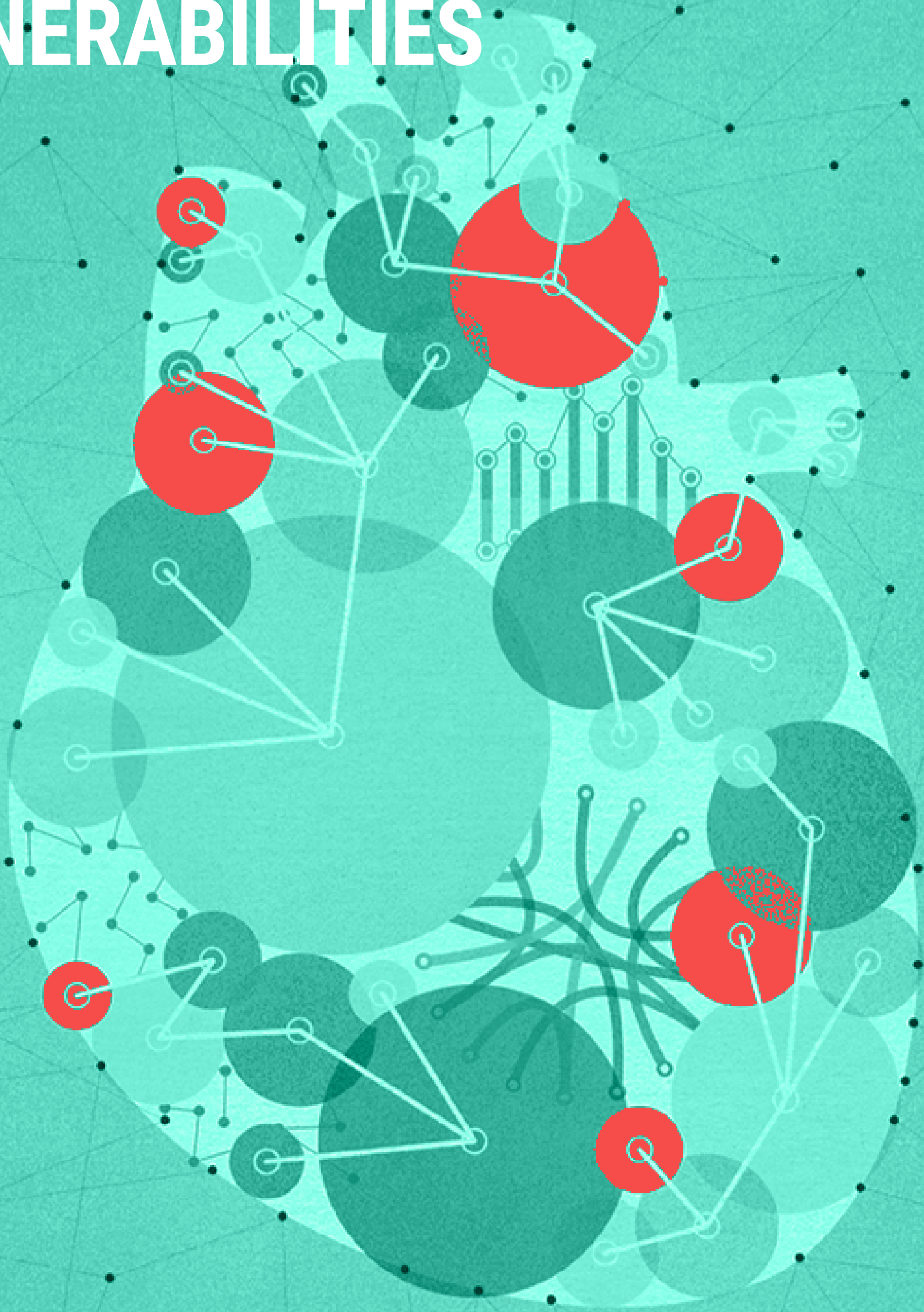
States should create procedurally transparent frameworks to assess whether and when to disclose not publicly known vulnerabilities or flaws they are aware of in information systems and technologies. The default presumption should be in favor of disclosure.

BACKGROUND

As the complexity of operating systems, critical software and computer hardware grows, they increasingly contain vulnerabilities. Those vulnerabilities can be exploited by state and non-state actors. States sometimes have conflicting interests and responsibilities when dealing with newly discovered vulnerabilities. On the one hand, they have an obligation to promote the resilience and integrity of infrastructure essential to the stability of cyberspace and by helping thwart malicious cyber activity make the entire digital ecosystem safer for all users. This would argue for a state to quickly disclose newly discovered vulnerabilities to vendors and manufacturers for patching, as well as making broader public disclosures, where appropriate, to protect the public. On the other hand, states have an obligation to protect their citizens from criminals, to investigate and prosecute cyber crime offenses, and reserve the right to impose sanctions that act as both a specific and a general deterrent to future malicious activity. An essential tool to pursue malicious actors, and particularly sophisticated actors such as rogue states, is the exploitation of vulnerabilities in the digital infrastructure on which they rely. States therefore often argue that they must preserve at least some select capabilities, including the use of undisclosed vulnerabilities, or else extremely capable malicious actors would go undiscovered and unchecked.

While states are unlikely to voluntarily disclose every vulnerability they discover, there has been a recent move by several states away from a presumption that all undisclosed vulnerabilities will be retained, to a presumption in favor of disclosure in the interests of greater systemic cybersecurity. A key part of this is the creation, by states, of a publicly described process for assessing the pros and cons of disclosure that takes into account the full range of policy, economic, social and technical equities. More specifically, that process should be procedurally transparent and take into account a full range of views including factors such as: network security and resiliency, the security of users and their data, law enforcement and national security utility, and diplomatic and commercial implications. The United States has recently promulgated a new version of such a process and other countries are considering creating their own Vulnerability Equities Process (VEP) policies. Given that vulnerability discovery and disclosure is broader than any one state, in order to promote network resilience while at the same time safeguarding national security, it would be in the interest of the long-term stability of cyberspace for every state to have such a process in place. Additionally, states should work towards compatible and predictable processes. The existence of such processes can act as a confidence-building measure between states in that it provides some assurance that relevant equities and competing interests are fully considered. Of course, every state has differing capabilities and unique interagency structures, however, any effective VEP process should be designed to take a broad range of perspectives and equities into account. In addition, though the actual decisions reached in individual cases may, out of necessity, remain confidential, there should be transparency on the general procedures and framework for reaching such decisions. Finally, this norm deals only with the establishment of a process where disclosure decisions are made. If a government or any other entity decides to make a disclosure, such disclosure should be made in a responsible manner that promotes public safety and does not lead to exploitation of that vulnerability.

6. NORM TO REDUCE AND MITIGATE SIGNIFICANT VULNERABILITIES



NORM:

Developers and producers of products and services on which the stability of cyberspace depends should (1) prioritize security and stability, (2) take reasonable steps to ensure that their products or services are free from significant vulnerabilities, and (3) take measures to timely mitigate vulnerabilities that are later discovered and to be transparent about their process. All actors have a duty to share information on vulnerabilities in order to help prevent or mitigate malicious cyber activity.

BACKGROUND

Certain IT products and services are essential to the stability of cyberspace due to their use within the core technical infrastructure, such as in core name resolution or routing, because of their widespread facilitation of the user Internet experience, or because of their use within critical infrastructures. Those creating products and services must commit to a reasonable level of diligence in the designing, developing, and delivering of products and services that prioritizes security and in turn reduces the likelihood, frequency, exploitability and severity of vulnerabilities.

Due to the increasing complexity of software and hardware, vulnerabilities in those products are a fact of life. While those vulnerabilities are usually unintentional, malicious state and non-state actors often exploit these vulnerabilities when discovered in ways that undermine the stability of cyberspace.

Moreover, in a hyper-connected and hyper-dependent world, a discovered vulnerability may affect multiple products and services by different producers and in different environments. Patching one product without disclosing the underlying vulnerability to others may protect that product but not protect the stability of cyberspace writ large. Those in the best position to assess the impact of a given vulnerability are often those who develop, produce, install or operate the products that the vulnerabilities affect. It is important to share information that would assist in fixing security vulnerabilities or help prevent, limit or mitigate an attack.[57]

While it is currently very difficult to ensure that no vulnerabilities exist in newly released or updated products, rather, this proposed norm suggests that those involved in the development or production of such products take “reasonable steps” that would reduce the frequency and severity of those that do occur.

Just as the “no tampering” norm addresses intentional insertion of vulnerabilities into critical products and services, and the hygiene norm ultimately addresses the duties of end users, this proposed norm seeks to have those who develop or produce critical products take reasonable measures to ensure that the number and scope of critical vulnerabilities are minimized and that they are effectively and timely mitigated and, when appropriate, disclosed when discovered. The process used should be transparent to create a predictable and stable environment.

[57] One of the norms for responsible behavior of states in the 2015 Report of the UN GGE (A/70/174) affirms that “States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure.”

7. NORM ON BASIC CYBER HYGIENE AS FOUNDATIONAL DEFENSE

NORM:

States should enact appropriate measures, including laws and regulations, to ensure basic cyber hygiene.

BACKGROUND

As Internet connectivity spreads around the world pervading all aspects of modern life, users of every kind—individuals, organizations, enterprises, and governments—are growing more and more reliant on technology and access to information available on the Internet. Politics, economics, public information, education, development and every other manner of social interaction depend critically on the Internet and associated technologies. Yet, this modern wonder remains broadly unsafe, and no one is immune to its dangers.

Consensus has yet to emerge on the most effective ways to optimize the promising technologies of cyberspace while safeguarding the public. Yet, most agree that the benefits of our digitally connected lives cannot be sustained going forward without agreed standards of essential security in cyberspace. To this end, the Commission strongly endorses the widespread adoption and verified implementation of basic cyber hygiene—a regime of foundational measures that represent prioritized, essential tasks to perform to defend against, prevent and rapidly mitigate avoidable dangers in cyberspace. Indeed, given the extensiveness of interconnectivity online, these measures constitute a basic duty of care that should be required of all users. Hygiene regimes should incorporate reliable measures of implementation, provide for widespread sharing of technical information and best practices, and be subject to appropriate oversight. Increasingly smart devices and processes demand smart laws and regulations. In creating more accountability for this basic duty of cyber care, governments should not curtail innovation or alter the basic properties of the Internet.

Cyber hygiene standards already exist in various forms.[58] They have been gaining wider international acceptance, as governments and enterprises increasingly understand the importance of taking steps demonstrated to help prevent and rapidly mitigate the dangers of known malware. Moreover, these standards represent best practice, highlight the importance of sensible, regular oversight and underscore the importance of automated information sharing where possible to alert other users to trouble. Such basic cyber defenses as outlined in these approaches account for the reality that no government, organization or collection of users can single-handedly alleviate all cyber-related risks. They also recognize that users at every level have important roles to play in strengthening cybersecurity.

The GCSC believes that fundamental cybersecurity defense through the widespread adoption of cyber hygiene has become essential to the responsible use and beneficial growth of the Internet. Security must be seen as a continuous process with responsibilities distributed among all actors with mechanisms in place, such as automated reporting and information sharing, to ensure appropriate accountability.

The Commission also recognizes that many societies around the world face considerable challenges in the use of information and communications technologies and calls on states to share knowledge and offer capacity building to instantiate processes for the effective implementation of basic cyber hygiene regimes to widen the effect of this norm.

[58] This includes, for example, by the European Telecommunications Standards Institute (ETSI), the not-for-profit Center for Internet Security (CIS) and the Australian Signals Directorate (ASD), among others.

8. NORM AGAINST OFFENSIVE CYBER OPERATIONS BY NON-STATE ACTORS

NORM:

Non-state actors should not engage in offensive cyber operations and state actors should prevent such activities and respond if they occur.

BACKGROUND

While information and communication technologies have positively transformed societies, they also pose new security challenges. The speed and ubiquity of cyber operations often poses considerable difficulties to states' judicial systems and international law enforcement cooperation. Despite these difficulties, it should be recalled that state sovereignty is the cornerstone of the rules-based international system of peace and security. States have a monopoly on the legitimate use of force, strictly bound by international law. Some non-state actors, mainly private companies, advocate for the right to conduct offensive cyber operations across national borders, potentially claiming that it constitutes a necessary defensive action as states do not have the capacity to adequately protect them against cyber threats. These non-state actors' offensive cyber operations are sometimes euphemistically referred to as "active cyber defense,"[59] including but not limited to so-called "hack back," as they are conducted for defensive purposes.

Some states do not control or may actively ignore these practices, despite the risk they impose upon the stability and security of cyberspace. However, in many states such practices would be unlawful, if not criminalized, while in other states they appear to be neither prohibited nor explicitly authorized. A few states are, nevertheless, considering legitimizing non-state actors' offensive cyber operations. Indeed, some have decided or proposed domestic legislation to allow offensive operations by non-state actors.

The GCSC believes that these practices undermine the stability of cyberspace. They can result in serious disruption and damages, including for third parties, and are thus likely to trigger complex legal disputes and escalate conflicts. States explicitly granting or knowingly allowing non-state actors the authorization to conduct offensive operations, for their own purposes or those of third parties, would set a dangerous precedent and risk violating international law. The Commission believes that offensive measures should be reserved solely to states and recalls that international law establishes a strict and exclusive framework for states' responses to hostile acts that also applies to cyber operations. Similarly, under international law, non-state actors acting on behalf of states must be considered their agents and are therefore considered extensions of the state.[60]

If states permit such action, they may therefore be held responsible under international law.[61] States must act, domestically and internationally, to prevent offensive cyber operations by non-state actors.

[59] Active cyber defense should be understood as a set of measures ranging from self-defense on the victim's network to destructive activity on the attacker's network. Offensive cyber operations within this continuum imply for the defender to act outside of its own network independently of their intention (offense or defense) and the legal qualification of their acts. Further work should be conducted on the definition of offensive cyber operations and active cyber defense.

[60] See "additional note" for a wider treatment of the case within international law, available here: https://cyberstability.org/wp-content/uploads/2018/11/Additional-Note-to-the-Norm-Against-Offensive-Cyber-Operations-by-Non-state-Actors-Norm-Package-Singapore.pdf.

[61] Id.

APPENDIX C: HISTORY, GOALS, AND PROCESSES OF THE GCSC

Since its launch at the February 2017 Munich Security Conference under the patronage of Dutch Minister of Foreign Affairs Bert Koenders, the Global Commission on the Stability of Cyberspace has been considered one of the first multistakeholder initiatives of its kind to specifically concentrate on the stability of cyberspace. Chaired by Michael Chertoff, former United States Secretary of Homeland Security; Latha Reddy, former Deputy National Security Advisor of India; and previously by Marina Kaljurand, Member of the European Parliament and former Foreign Minister of Estonia, the Commission comprises 28 prominent individuals from different geographies as well as different backgrounds related to international cybersecurity.[62] It is supported by Special Advisors, a Secretariat, comprised of *The Hague* Centre for Strategic Studies and the EastWest Institute, a Research Advisory Group, as well as a number of partners and sponsors, including the Ministry of Foreign Affairs of the Netherlands and France, the Cyber Security Agency of Singapore, Microsoft, the Internet Society, and Afilias.

The Commission was born from the desire to continue the work of previous civil society commissions, including the Global Commission on Internet Governance, and to connect to the work of the Global Conference on CyberSpace (GCCS). In 2015, *The Hague* Centre for Strategic Studies (HCSS) was asked to organize a preparatory session for The Hague meeting of the GCCS, dedicated to international peace and security. Much of the subsequent GCCS declaration drew directly on the work of the preparatory meeting, clearly outlining the need for a multistakeholder format to discuss international cybersecurity issues. Accordingly, HCSS convened a core group of supporters and funders (originally Microsoft, the Internet Society, and the Ministry of Foreign Affairs of the Netherlands) and developed a strategic plan. In August 2016, having gained the EastWest Institute (EWI) as a partner in the Secretariat, HCSS convened a meeting of the GCSC Inception Group at Harvard Kennedy School, which drafted the main requirements for both the operation of the GCSC, its membership, structure, and goals, as well as its mission statement.

The mission statement reads:

> The Global Commission on the Stability of Cyberspace (GCSC) will develop proposals for norms and policies to enhance international security and stability and guide responsible state and non-state behavior in cyberspace. The GCSC will engage the full range of stakeholders to develop shared understandings, and its work will advance cyberstability by supporting research, information exchange, and capacity building.

From its start, the GCSC was intended to influence the international peace and security agenda related to cyberspace, generally referred to as

[62] See full list of Commissioners on page 4.

"international cybersecurity." The Inception Group identified a need to solicit diverse views, especially from the Internet governance and technical communities, into the ongoing international cybersecurity discussions. The goal was to better inform the deliberations in the arms control and peace and security communities, where much of the good work, particularly on norms, was considered hampered by the lack of input and acceptance from these civil society and private sector actors. The multistakeholder approach was therefore considered to be a practical rather than an ideological issue.

The GCSC approached its deliberations in a "bottom-up to top-down" manner. Firstly, it identified operational norms that meet the most obvious urgent international cybersecurity needs as expressed by its members and which have not been addressed elsewhere. Secondly, it extrapolated from these and already existing norms a working definition of cyberstability and its underlying principles. Thirdly, a stability framework was developed for a clearer understanding of what the international peace and security architecture needs to do to meet that definition. Lastly, it developed recommendations addressed to state and non-state stakeholders on how this could be accomplished.

The deliberations of the Commissioners towards these goals were conducted across geographical boundaries and across stakeholder groups. From the start, the Commission put the emphasis on holding its meetings in the margins of relevant conferences to facilitate input from a wide range of stakeholders.[63] It also actively solicited input through research and from the wider community. To connect the work of the GCSC to the wider academic community, the Research Advisory Group was instigated with a chair and four deputy chairs[64] responsible for managing an email list of over 200 experts. It was also the basis for a wide-ranging research program, which eventually commissioned over 20 studies from research institutions and individuals worldwide.[65] The bulk of this work was presented directly to the Commissioners at the dedicated "CyberStability Hearings."

Prior to the publication of this report and the previously issued norms, the Commission consistently sought input from a broad range of government, civil society, and industry stakeholders. By staggering the delivery over the entire tenure of the Commission it was possible to constantly invite outside input and comment. Online Requests for Consultations were issued on the GCSC norms and the definition of cyberstability. Over 23 submissions were received from actors worldwide which went towards informing the deliberations of the Commissioners. Furthermore, the Commission actively participated in more than 70 conferences and events, and convened roundtables, side-events, and dedicated CyberStability Hearings with a wide range of state and non-state stakeholders.

Finally, the Commissioners themselves maintained active links with their own respective communities. Input and feedback from these groups represented the bedrock of interactions with the wider community of state and non-state experts and will form the basis of the advocacy of the report going forward.

[63] Official meetings of the Commission were convened at the following events: 2017 Munich Security Conference (Munich, Germany); CyCon (Tallinn, Estonia); BlackHat USA (Las Vegas, USA); Global Conference on CyberSpace (New Delhi, India); 2018 FIC International Cybersecurity Forum (Lille, France); 2018 Munich Security Conference (Munich, Germany – Conferral); GLOBSEC (Bratislava, Slovakia); Israel Cyber Week (Tel Aviv, Israel – Conferral); Singapore International Cyber Week (Singapore); Paris Peace Forum & IGF (Paris, France – Conferral); 2019 United Nations Institute for Disarmament Research (Geneva, Switzerland); ICANN 64 Community Forum (Kobe, Japan); EuroDIG (The Hague, Netherlands); GFCE Annual Meeting (Addis Ababa, Ethiopia).

[64] Covering four topic areas, including international peace and security, international law, Internet governance, and technology.

[65] See Acknowledgements section.

ACKNOWLEDGEMENTS

The Global Commission on the Stability of Cyberspace (GCSC) would like to thank the many institutions and individuals who supported, contributed to, and facilitated the work of the Commission including, but not limited to our sponsors, Research Advisory Group, research paper authors and peer reviewers, and support staff. Below are just a few of those who contributed to the success of the Commission.

Secretariat

THE HAGUE CENTRE FOR STRATEGIC STUDIES (HCSS)

Alexander Klimburg, Director, Global Commission on the Stability of Cyberspace Initiative and Secretariat
Louk Faesen, Project Manager, Global Commission on the Stability of Cyberspace Secretariat
Elliot Mayhew, Project Assistant, Global Commission on the Stability of Cyberspace Secretariat

With additional support from: **Timon Domela Nieuwenhuis Nyegaard**, **Koen van den Dool**, **Niels Renssen**, and **Kaja Karlson**.

EASTWEST INSTITUTE (EWI)

Bruce W. McConnell, Co-Director, Global Commission on the Stability of Cyberspace Secretariat
Anneleen Roggeman, Project Manager, Global Commission on the Stability of Cyberspace Secretariat

With additional support from: **Abagail Lawson**, **Dragan Stojanovski**, and **Conrad Jarzebowski**.

Partners, Sponsors, and Supporters

The Hague Centre for Strategic Studies, the EastWest Institute, and the Commissioners would like to recognize and acknowledge the following organizations for their support:

PARTNERS:

- **Ministry of Foreign Affairs of the Netherlands**, **Timo Koster** and **Dimitri Vogelaar**
- **Microsoft**, **Jan Neutze** and **Kaja Ciglic**
- **Cyber Security Agency of Singapore**, **David Koh** and **Sithuraj Ponraj**
- **Internet Society (ISOC)**
- **Ministry of Foreign Affairs of France**, **Henry Verdier** and **David Martinon**
- **Afilias**, **Ram Mohan** and **Philipp Grabensee**

SPONSORS:

- **Federal Department of Foreign Affairs of Switzerland**
- **GLOBSEC**
- **Ministry of Foreign Affairs of Estonia**
- **Ministry of Internal Affairs and Communications of Japan**

SUPPORTERS:

- **African Union Commission**
- **Black Hat USA**
- **DEF CON**
- **European Union Delegation to the UN in Geneva**
- **Global Forum on Cyber Expertise**
- **Google**
- **Municipality of The Hague**
- **Packet Clearing House**
- **Tel Aviv University**
- **United Nations Institute for Disarmament**

These organizations and institutions are committed to advancing the debate and putting forward creative solutions to some of the most pressing challenges facing the stability of cyberspace.

Researchers

The Commission would like to thank the members of its Research Advisory Group, a group of over 200 online members that connected the GCSC to the wider academic community. In particular, we would like to thank the researchers who were commissioned to write briefings and memos to inform the deliberations of the Commissioners.

GCSC ISSUE BRIEF 1 (NOVEMBER 2017)

Alex Grigsby, Formerly of the Council on Foreign Relations (CFR)
Deborah Housen-Couriel, Konfidas Digital Ltd.
Joanna Kulesza, University of Lodz and **Rolf H. Weber**, University of Zürich
Oluwafemi Osho, **Joseph A. Ojeniyi**, and **Shafi'i M. Abdulhamid**, Federal University of Technology, Minna
Analía Aspis, University of Buenos Aires
Robert Morgus, Formerly of New America, **Max Smeets**, Formerly of the Center for International Security and Cooperation, Stanford University, and **Trey Herr**, Harvard Kennedy School
Arun Mohan Sukumar, **Madhulika Srikumar**, and **Bedavyasa Mohanty**, Observer Research Foundation (ORF)

GCSC ISSUE BRIEF 2 (MAY 2018)

Shen Yi, **Jiang Tianjiao**, and **Wang Lei**, Research Center for the Governance of Cyberspace, Fudan University
Elana Broitman, **Mailyn Fidler**, and **Robert Morgus**, Formerly of New America
Elonnai Hickok and **Arindrajit Basu**, Centre for Internet and Society
Thomas Uren, **Bart Hogeveen**, and **Fergus Hanson**, Australian Strategic Policy Institute (ASPI)
Dragan Mladenović and **Vladimir Radunović**, DiploFoundation
Thomas Reinhold, Institute for Peace Research and Security Policy, University of Hamburg

Consultations

The Commission would like to thank the following individuals and organizations for submitting extensive comments in response to the Request for Consultations on the Singapore Norm Package (from 17 December 2018 until 17 January 2019) and the Definition of Stability of Cyberspace (from 14 August 2019 until 6 September 2019):

Hussein Abul-Enein, Access Partnership
Kayode Akanni, DesignIT
Jonathan D. Aronson, University of Southern California (USC)
Aviram Atzaba, Israel National Cyber Directorate
Arindrajit Basu, **Gurshabad Grover**, **Elonnai Hickok**, and **Karan Saini**, Center for Internet & Society
Vytautas Butrimas, NATO Energy Security Centre of Excellence
Cybersecurity Tech Accord
Michael Daniel, Cyber Threat Alliance
Global Partners Digital
Arvind Gupta and **Dickey Kumar**, Vivekananda International Foundation
Tara Hairston and **Anastasiya Kazakova**, Kaspersky
Sven Herpig, Stiftung Neue Verantwortung
Drew Mitnick, Access Now
George M. Moore, James Martin Center for Nonproliferation Studies
Brett van Niekerk and **Trishana Ramluckan**, University of KwaZulu-Natal
Peter Swire, **Justin Hemmings**, and **Sreenidhi Srinivasan**, Georgia Tech Scheller College of Business
Johan de Wit, Siemens/TU Delft

Finally, the Commission would like to thank the following experts, whose work and expertise have guided and informed the deliberations of the Commission:

Dennis Broeders, Leiden University
Deborah Brown and **Verónica Ferrari**, Association for Progressive Communications
Michael Daniel, Cyber Threat Alliance
François Delerue, Institut de Recherche Stratégique de l'École Militaire – IRSEM
Akhil Deo and **Arun Mohan Sukumar**, Observer Research Foundation (ORF)
Martha Finnemore, George Washington University
Aude Géry, University of Rouen
Duncan Hollis, Temple Law School
Joanna Kulesza, University of Lodz
Peter Rowland, Packet Clearing House
Michael Schmitt, Exeter Law School

Patra Kongsirimongkolchai / EyeEm / Getty Images

SECRETARIAT

The Hague Centre for Strategic Studies

EastWest Institute

PARTNERS

Ministry of Foreign Affairs of the Netherlands

CSA Singapore

Liberté • Égalité • Fraternité
République Française
Ministère de l'Europe et des Affaires Étrangères

Internet Society

Microsoft

Afilias

SPONSORS

Federal Department of Foreign Affairs of Switzerland

GLOBSEC

Ministry of Foreign Affairs of Estonia

Ministry of Internal Affairs and Communications of Japan

SUPPORTERS

African Union Commission

Black Hat USA

DEF CON

European Union Delegation to the UN in Geneva

Global Forum on Cyber Expertise

Google

Municipality of The Hague

Packet Clearing House

Tel Aviv University

United Nations Institute for Disarmament Research

GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE