Cyberstability Paper Series

New Conditions and Constellations in Cyber

December 2021

Edited by Alexander Klimburg

The Hague Centre for Strategic Studies

Cyberstability Paper Series
New Conditions and Constellations in Cyber

This publication may be cited as:
Alexander Klimburg (Ed.), New Conditions and Constellations in Cyber, The Hague Centre for Strategic Studies, The Hague 2021.

ISBN: 9789492102874

Co-editor: Louk Faesen
Reviewers: Alexander Klimburg, Louk Faesen, Tim Sweijs, Frank Bekkers

The Hague Centre for Strategic Studies

HCSS helps governments, non-governmental organizations and the private sector to understand the fast-changing environment and seeks to anticipate the challenges of the future with practical policy solutions and advice.

The Hague Centre for Strategic Studies
Secretariat of the Global Commission on the Stability of Cyberspace
info@hcss.nl hcss.nl
Lange Voorhout 1
2514EA The Hague
The Netherlands

Since the release of the final report of the Global Commission on the Stability of Cyberspace in November 2019, the concept of cyberstability has continued to evolve. A number of new 'conditions' are emerging: new agreements on norms, capacity building and other stability measures have been proposed and solidified within the United Nations and elsewhere, and stakeholders are exploring ways to increase stability and minimize the risk of conflict in cyberspace through technical fixes or governance structures. The constellations of initiatives involved in working towards cyberstability is expanding, underlining the need to connect the traditional state-led dialogues with those of the Internet communities from civil society and industry. Gaps continue to close, between the global north and south, between technology and policy, but also the stability in and the stability of cyberspace.

The first Cyberstability Paper Series explores these "New Conditions and Constellations in Cyber" by collecting twelve papers from leading experts, each providing a glance into past or future challenges and contributions to cyberstability. The papers were released on a rolling basis from July until December 2021 and compiled in this edited volume. All papers are available for open access, and a limited number of printed hardback copies are available.

Contents

Foreword

Joseph S. Nye, Jr. | Harvard University Distinguished Service Professor, Emeritus

Today, the world is living through an information revolution as profound as that which followed Gutenberg's invention of the printing press in the 15th century, and it is important to remember that Gutenberg's revolution was followed by insecurity and instability that tore European societies apart. The Internet has existed since the 1970s, but only in this century have computer networks become a vital part of the global economy. At the beginning of the century, only a few percent of the world's people were online. Now, with the spread of the World Wide Web, mobile phones, and social media, more than half the world population relies on the Internet.

The Internet has become an essential substrate for economic, social, and political interactions. The good news is that connectivity produces efficiency and economic gains, but the bad news is that it also produces vulnerability and insecurity. With big data, artificial intelligence, advanced robotics, and the "Internet of Things," the number of cyber connections may approach a trillion by 2030. The world has experienced cyberattacks since the 1980s, but the attack surface has expanded dramatically and now includes everything from industrial control systems to automobiles to personal digital assistants. In terms of global peace and prosperity, we have to ask how we can engender stability in cyberspace.

In terms of global military conflict, computer networks have become a fifth domain in addition to the traditional four, of land, sea, air, and space. Many countries have established specialized cyber command units. Among the special characteristics of the new cyber domain are the erosion of distance; speed of interaction; low cost, which reduces barriers to entry; and difficulties of attribution, which promote deniability and slow responses to attacks. Both states and non-state actors have become attackers as well as defenders.

Societies take time to learn how to respond to major disruptive technological change. For example, nuclear technology burst into public consciousness after Hiroshima in 1945, but in terms of chronology it took more than two decades before states began to reach the first norms and agreements by which to control nuclear weapons. If we start from the time that the Internet became broadly commercialized, cooperation in developing cyber norms is now approaching such a two-decade mark. In 1998, Russia first proposed a UN treaty to ban electronic and information weapons. The US rejected the treaty as unverifiable, because whether a line of code is a weapon or not can depend on the changeable intent of the user.

Joseph S. Nye Jr. is University Distinguished Service Professor, Emeritus and former Dean of the Harvard's Kennedy School of Government. He has served as Assistant Secretary of Defense for International Security Affairs, Chair of the National Intelligence Council, and Deputy Under Secretary of State for Security Assistance, Science and Technology. He is a Commissioner on the Global Commission on the Stability of Cyberspace.

Instead, the UN Secretary General appointed a group of governmental experts (GGE), which first met in 2004. Six GGEs have convened since then and issued four reports, most recently in June 2021. The 2015 report agreed on eleven voluntary norms, most importantly not attacking civilian infrastructure, not interfering with computer emergency response teams, not allowing one's territory to be used for wrongful acts, and providing assistance when requested. These norms were reinforced in 2021 by the report of an Open-Ended Working Group of all UN members, which also stated that existing international law applies in the cyber domain.

In addition to the UN process, there have been many sources of suggestions about cyber norms. In the OEWG negotiations, one of the most mentioned initiatives was proposed by the Global Commission on the Stability of Cyberspace (GCSC), described in these pages. Initiated by a Dutch think tank with strong support from the Dutch government, the GCSC had co-chairs from Estonia, India, and the United States, an able international staff, and was comprised of former government officials, experts from civil society, and academics from sixteen countries. It developed eight norms with which to address what we saw as gaps in those previously declared by the GGE, including a norm for protecting the "public core" backbone infrastructure of the global Internet from attack, as well as prohibiting interference with electoral systems, to name two of the most prominent examples. Other norms proposed by the commission included not interfering with supply chains; not introducing cyber robots into others' machines; creating transparent processes for judging whether to disclose flaws and vulnerabilities discovered in coding; encouraging prompt patching; improving cyber hygiene; and discouraging private vigilantism, or "hack-back." Another multistakeholder initiative, the French-led Paris Call for Trust and Security in Cyberspace, adopted six of the GCSC norms in 2019. Many further norms can be imagined and have been proposed for building stability in cyberspace, but the important question now is not more norms but whether they will alter state and non-state actors' behavior.

A regime of cyber norms will be essential if we are to avoid the ongoing deterioration of international order that will otherwise accompany the rapid technological changes described above.

Skeptics dismiss these voluntary peacetime norms, but violation does not make norms irrelevant, either at the domestic or international level. Norms create expectations about behavior that make it possible to hold other states and non-state actors accountable. Norms help legitimize enforcement actions. From a longer historical perspective, a regime of cyber norms will be essential if we are to avoid the ongoing deterioration of international order that will otherwise accompany the rapid technological changes described above. As they approach the chapters that follow, readers should realize that norms alone are not sufficient to prevent such instability, but they will be necessary.

Preface

Latha Reddy and **Michael Chertoff** | Co-Chairs of the Global Commission on the Stability of Cyberspace

Cyberspace is a domain of constant change. As such, it requires agile, not static, mechanisms by which to ensure stability as the world changes around it. Cyberstability therefore means that new conditions and constellations must be able to emerge. This Paper Series contributes to the understanding of these new aspects of cyberstability.

The mission of the Global Commission on the Stability of Cyberspace (GCSC), which we had the honor of co-chairing, was to help advance cyberstability by proposing norm and policy initiatives that helped advance stability in cyberspace.[1] We are very proud that the GCSC is widely considered to have been a success, including also in academic literature.[2] However, while this success is currently mostly measured against our influence on the evolving debates on norms and soft law with the United Nations First Committee dealing with disarmament and International security, we believe that our influence on the definition of what actually constitutes cyberstability will be at least as important, and potentially longer lasting.

Definitions of cyberstability will evolve with the domain itself. This Series can, of course, never offer more than a snapshot of the many topics that together help define stability in cyberspace. It is also therefore by necessity a highly diverse collection of views—going beyond a focus on international peace and security to include voices from international development, Internet governance, the rights communities, and also from the technical heart of the Internet. We believe that this diversity of views, like the diversity of the makeup of the GCSC, are a strength, not a weakness. It can help break silos on thinking and introduce some urgently needed mutual understanding and coherence between the different strands of cyberstability. Each strand can in turn be strengthened by learning from others and, while maintaining its own unique voice and identity, continue to craft solutions that take a holistic view of cyberstability to heart. Diversity does not mean ignorance of the other, but mutual respect and recognition, and working through common values of principles toward a shared goal. An approach rooted in diversity also grows stronger when new voices and experts are added. We hope that with this Collection we can add additional voices, and continue to work together in our common goal to strengthen the stability of cyberspace.

1 "Open-ended Working Group," https://www.un.org/disarmament/open-ended-working-group/; "Group of Governmental Experts," https://www.un.org/disarmament/group-of-governmental-experts/; "Paris Call for trust and security in cyberspace," https://pariscall.international/en/

2 Jacqueline Eggenschwiler, "Expert commissions and norms of responsible behaviour in cyberspace: a review of the activities of the GCSC," Digital Policy, Regulation and Governance 22, no.2 (May 2020): 93-107 https://doi.org/10.1108/DPRG-03-2019-0019

Latha Reddy is Co-Chair of the Global Commission on the Stability of Cyberspace. She is the former Deputy National Security Adviser of India, where she was responsible for cybersecurity and other critical internal and external security issues. Previously she also served as a Commissioner on the Global Commission on Internet Governance.

Michael Chertoff is Co-Chair of the Global Commission on the Stability of Cyberspace. He served as Secretary of the U.S Department of Homeland Security (DHS) from 2005 to 2009. Before DHS, he served as a federal judge and as a federal prosecutor. He is also the Co-founder and Executive Chairman at the Chertoff Group.

Introduction

Alexander Klimburg, PhD | Director, Global Commission on the Stability of Cyberspace Initiative and Secretariat

Cyberstability represents an ideal state, one that may require constant effort to attain. As such, it requires continuous new input. This collection of essays is an attempt to drive that understanding further.

In a recent US State Department paper on the term "strategic stability," the author concluded that the phrase was a "descriptive term rather than a normative term: it [is] less a per se good than something that is good or bad, desirable or undesirable, depending upon the circumstances and upon the values that one prizes."[1] The term cyberstability, like its cousin cyber peace,[2] is the opposite of this: it is wholly normative, sketching an ideal state that does not yet exist. It is therefore an ongoing work in progress.

The Global Commission on the Stability of Cyberspace (GCSC), of which I had the privilege of serving as its director, defined cyberstability as a state in which "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."[3]

This definition appeared in the November 2019 GCSC Final Report, "Advancing Cyberstability," for the first time. It helped introduce one of the main deliverables of the GCSC: the Cyberstability Framework. This framework included the key issues that needed to be considered in the pursuit of cyberstability: multistakeholder engagement, adherence to international law, open technical standards, a set of cyberstability principles, capacity building, confidence-building measures, and voluntary norms. The Commission made a primary contribution to three items of the framework, namely, the principles, the role of the multistakeholder approach, and norms. Indeed, many of the eight norms proposed have gone on to have a significant impact in the global discussion on peace and security in cyberspace, and some, such as the norms against non-interference with the public core of the Internet, have been widely supported, both in spirit, and, sometimes, in letter. Despite the success of many of the GCSC norms, it is the contribution to the evolving definition of cyberstability that may yet prove to be the most influential.

The GCSC did not start its work by defining cyberstability, but rather arrived at its definition based on its work, itself guided from the start by its mission statement "to develop norms and policy initiatives that advance international security and stability." Crafting a definition at the end rather than in the beginning of a deliberative process is wholly in-line with the growth of cyberspace and the Internet itself, whose bottom-up and end-to-end characteristics have meant that development has

Alexander Klimburg is the Director of the Global Commission on the Stability of Cyberspace Initiative and Secretariat, and the Director of the Cyber Policy and Resilience Program at The Hague Centre for Strategic Studies. He is also a Senior Associate at the Center for Strategic and International Studies (CSIS) and an Associate Fellow at the Austrian Institute of European and Security Policy.

gone before grand design, and where growth has been above all organic, and not forced or guided by anything else then practical considerations. This means that cyberspace and the Internet will be in constant change—ideally "one managed in relative peace"—and likewise this means that exactly what constitutes cyberstability will change as well.

Since the release of the final GCSC report in November 2019, the concept of cyberstability has continued to evolve. A number of new "conditions" are emerging: new agreements on norms, the rise of capacity building as a distinct line of effort, and ideas for new confidence with other stability-building measures have crystalized. Other developments, such as the instating on the so-called digital cooperation discussion, and also attempts to advance a counter cybercrime convention within the UN, have had a mixed reception. Overall, the constellation of cyber initiatives is expanding, underlining that, even if it is not always necessary to connect everything with each other, it is always important to strive for mutual coherence.

This is especially so between the traditional state-led dialogues on international security and the non-state led field of Internet governance. The former considers issues of "use" of the Internet and the latter concerns itself with "development" of the Internet (according to the seminal Tunis Agreement of the UN World Summit of the Information Society (WSIS)),[4] and both have equally different constituents. According to the Tunis Agreement, non-state actors lead the development of the Internet, while the use of the Internet is today increasingly decided by states. There is also a clear ideologically split, where some governments insist that the use of the Internet must guide its development, therefore attempting to assert primacy over the non-governmental-led Internet. As described above, however, the Internet has always put development first—where decisions made on the margins have determined its growth, rather than the specific top-down planning by governments or large companies.

The GCSC was primarily concerned with the use of the Internet—the international peace and security agenda related to cyberspace, generally referred to as international cybersecurity. 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 civil society and private sector actors. However, the use of the Internet does to a certain extent also depend on its development, and, while the GCSC did not seek to influence Internet governance, it sought to port its concerns and considerations into the international security realm. Perhaps the most defining aspect of this is the rooting of Internet governance in a multistakeholder model, which is indelibly connected with the bottom-up and end-to-end nature of the global Internet. The multistakeholder approach was therefore considered to be a practical rather than an ideological issue, and the GCSC was committed to exploring to what extent it could be better introduced to the UN First Committee processes that define the international cybersecurity debate. The rationale was that a plurality of competent views from differing backgrounds would be an unalloyed good in helping the diplomats craft better agreements. The same rationale also applied in helping to deepen the definition of what constitutes cyberstability, which is the focus of this paper series.

Despite the success of many of the GCSC norms, it is the contribution to the evolving definition of cyberstability that may yet prove to be the most influential.

Within the state-led discussions on international security in cyberspace, there have been two notable recent achievements. The UN Open-Ended Working Group (OEWG) and the Group of Governmental Experts (GGE), previously described as two competing processes, managed against all odds to deliver consensus reports, after the GGE failed to do so in 2017. In her paper, Tiirmaa-Klaar

delves into the history of the GGE, offering a peek behind the curtain and the success factors that, over fifteen-odd years, turned a relatively marginal UN group into the central cyber rules-setting body and vehicle for multilateral consensus. Among the key factors for success were the people driving the process, most recently the Chairs of both UN groups—one of whom also contributed to this volume. In his article, OEWG Chair Lauber—together with Lukas Eberli—offers unique insights into this process and how it was able to move away from confrontation to consensus, to find complementarity with the GGE, and how it was able to reaffirm the existing cyber acquis. The OEWG also opened a new chapter of non-governmental involvement in the traditionally state-led discussions of the UN First Committee. There is still room for improvement, as involvement of civil society and industry mostly occurred on an informal basis and largely depended on the ECOSOC accreditation. Nonetheless, there is no more denying non-governmental stakeholders a seat at the table, and we can look forward to the multistakeholder element of cyberstability, which may (borrowing from Henry Kissinger) be considered the new "legitimizing principle" of the cyber age,[5] advancing further in international security.

What appropriate involvement by non-governmental stakeholders can look like in the upcoming OEWG is a question further addressed by Kleinwächter, who sketches out three ways to enhance multistakeholder cooperation, namely, informal consultations, speaking rights in regular sessions, and the establishment of a non-state advisory committee. Teasing out the importance of this new multistakeholder cooperation also plays an important role in Esterhuysen and Degezelle's history of the Internet Governance Forum (IGF). Having provided the largest, most diverse and inclusive platform for open dialogue on internet-related policy issues for over fifteen years, the Forum also faces criticism for being just a "talk-shop." Faced with numerous proposals to change its mission, and with the renewal of its mandate scheduled in 2025, the authors believe in a delicate balance between, on the one hand, staying the same—retaining its bottom-up and open character— and, on the other hand, changing, taking risks, opening up to new and different voices and interests, and interrogating the status quo.

McPherson combines a close look at how the private sector and civil society actually manage the Internet, in a briefing on the critical topic of routing security. He shows how the Resource Public Key Infrastructure, a key evolving protocol for routing security, needs to be included in any future work on the public core. However, in order to build technical cybersecurity for countries around the globe, thereby achieving a more inclusive and coherent international set of international cyber policies, there is a need for more capacity building. Despite the many international initiatives and commitments, Painter finds that cyber capacity building is under-resourced and under-prioritized. He offers recommendations for promoting it as a global priority, both within and outside of the UN, to increase resources and link it to the SDGs and OECD DAC, and finally to strengthen coordination mechanisms through the GFCE and by leveraging regional efforts.

One important component of cyberstability is the respect for human rights. It is one of the four GCSC principles (next to responsibility, restraint, and the requirement to act) that inform cyber norms and policies. Owiny and Kumar focus on the effects of Internet shutdowns in the Democratic Republic of the Congo, Tanzania, and Uganda on the cyberstability principles. Not only do these shutdowns violate all four principles, they also are in violation of international law, in particular human rights such as freedom of expression, the right to work, and the right to access information, and could harm international relations. Taking an economic track, Ndemo explores the relationship between digital transformation and cyberstability in Africa, arguing that the latter is essential for the continent's short- and long-term economic development and sustainability. Digitalization holds enormous potential to this end—a 10% increase in mobile-internet penetration can increase GDP

capita by 2.5% in Africa as opposed to only 2% in the rest of the world. While some African countries were early adopters and leapfrogged in certain areas, others lag behind and barriers remain, ranging from weak national education, political intolerance, to uneven distribution of infrastructure development in rural and urban centers. Ndemo urges countries to embark on human-resource development, to expand employment opportunities, and to democratize access to supporting infrastructure and products.

In a further sign of the potential of the Global South in cyber, Reddy and Soni outline the independent role that the Non-Aligned Movement (NAM) could have in digitalization, especially working together with the European Union. A joint 5G Initiative is proposed to help de-escalate a burgeoning Digital Cold War. Further, the Initiative could lead to the establishment of a Digital Stability Board—modeled around the existing Financial Stability Board—that can act as a coordination body for best practices and standards.

For any new norm, be it organizational or simply one of practice, to be effective there must be consequences for transgressions. This connects back to the criticism of the "soft law" approach laid out by the UN GGE, where norms violators must be deterred from transgressing. Daniel finds that the problem for cyber deterrence is not whether it works against serious cyberattacks—which he clearly believes it does—but whether it can be expanded to work against a broader set of cyber activities well beneath the threshold of armed conflict. Our mental models that are based on the physical world do not work well for cyberspace and need to be revised, including reconceptualizing the role of non-governmental actors in international cybersecurity. A new policy design for expanded deterrence would define the new activity to be deterred, make use of comparative advantages, link cyber issues with non-cyber issues, encompass more than technical cyber actions, and involve active disruption.

While Daniel explores some of the main priorities of the Western like-minded states, Xu Peixi goes into the Chinese perspective of cyberspace, by exploring the evolution of the notion of security in China. Influenced by Confucian and Taoist traditions, China views cyberspace both as an external source of threat to Chinese integrity, and as a crucial element for boosting its predominantly digital economy. The author finds that a good-vs-bad-guys perspective is not useful and instead argues that all societies and cultures have both authoritarian and libertarian orientations in handling the mixed security and development challenges posed by cyberspace. Norms have been and remain an important tool with which to reach global consensus and avoid further fragmentation and isolation between different camps.

Government and non-state experts are now shifting their focus to finding ways to implement, enforce, and advance the rules of the road. To do so, they are looking back at history to identify potential lessons transferrable to cyberspace. One such example is the Incidents at Sea Agreement (INCSEA) that signified a milestone in confidence building, de-escalation, and avoiding inadvertent escalation at sea during the Cold War. In a Pro/Contra paper, two views were sought on the matter. One the one hand, Bahney, Reiber, and Williams believe INCSEA is a poor model for cyberspace, in no small part due to widely different geopolitical conditions. Neither does it fit the operational realities of cyberspace, nor could it address the key policy and stability challenges related to cybersecurity. Klimburg, on the other hand, approaches INCSEA as a thought-experiment that transposes the original articles of the agreement directly to cyber. Despite some challenges in terms of definitions, scope, and especially political will, a direct transposition shows how little a barrier some of these challenges really are, and that the original INCSEA agreement has a lot to offer. In

particular, using the existing body of cyber norms as a starting point, it could prove to be a useful confidence-building measure of its own.

These essays offer a widely differing set of inputs on a commonly perceived problem—social and political insecurity and instability driven by specific factors associated with the use of the Internet. Despite their various backgrounds, the accomplished authors all address issues that align with the definition of cyberstability put forward by the GCSC. Indeed, so wide is the breadth of issues covered that few readers will be equally attuned to all of the topics covered here. This is an unalloyed good—for only by advancing our understanding of different aspects of cyberstability will we be able to advance this common vision.

Endnotes

1 Christopher A. Ford, "Strategic Stability and the Global Race for Technology Leadership," Arms Control and International Security Papers 1, no. 21 (November 2020). Available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwi4qfSXs7H0AhXFg_0HHTjZCr0QFnoECAYQAQ&url=https%3A%2F%2Fwww.state.gov%2Fwp-content%2Fuploads%2F2020%2F11%2FT-paper-series-Strategic-Stability-and-Tech-508.pdf&usg=AOvVaw0qXlUEL8Kz4K9t5839iy9g

2 The terms "cyberstability" and "cyber peace" have often been assigned to different ideological and political corners, however in recent years a noticeable convergence has occurred. See Alexander Klimburg and Virgilio A. F. Almeida, "Cyber Peace and Cyber Stability: Taking the Norm Road to Stability," IEEE Internet Computing 23, no. 4 (July-August 2019): 61-66. Available at: https://ieeexplore.ieee.org/document/8874985

3 The Global Commission on the Stability of Cyberspace, "2. What Is Meant By The Stability Of Cyberspace?," Cyberstability.org, available at: https://cyberstability.org/report/#2-what-is-meant-by-the-stability-of-cyberspace

4 World Summit on the Information Security, "Tunis Agenda for the Information Security", ITU, November 18, 2015, available at: https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html

5 Alexander Klimburg and Louk Faesen, "A Balance of Power in Cyberspace," in Governing Cyberspace: Behavior, Power, and Diplomacy, ed. By Dennis Broeders and Bibi van den Berg (London: Rowman & Littlefield International, 2020): 145-171.

Cyberstability Paper Series
New Conditions and Constellations in Cyber

The Evolution of the UN Group of Governmental Experts on Cyber Issues

From a Marginal Group to a Major International Security Norm-Setting Body

Heli Tiirmaa-Klaar
Ambassador for Cyber Diplomacy, Estonian Ministry of Foreign Affairs

The Evolution of the UN Group of Governmental Experts on Cyber Issues from a Marginal Group to a Major International Security Norm-Setting Body

Heli Tiirmaa-Klaar | Ambassador for Cyber Diplomacy,
Estonian Ministry of Foreign Affairs

This article offers insights on the major milestones and discussions by the consecutive United Nations Groups of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security. In parallel to addressing the development of cyber norms, the article also analyzes other pertinent regional and global developments during the period 2005–2021, which have formed the geostrategic context for the successive GGEs. It highlights the internal factors and external events that were at play in transforming this relatively marginal UN group in the early 2000s into a central cyber norm-setting body by 2021.

This article offers a depiction of nascent multilateral negotiations on cyber norms by the UN Groups of Governmental Experts to develop the framework for state behavior in cyberspace, which eventually becomes a widely accepted universal rulebook. Against the background of growing concerns stemming from misuse of new technologies to countries' foreign policy and national security, the story of cyber GGEs entails useful lessons for diplomats, decision-makers, and the larger public on how to achieve multilateral agreements on frontier issues of international security.

In summary, the GGEs achieved consensus when taking place during a favorable geopolitical context, where tensions between the leading powers were relatively low or there was otherwise

Heli Tiirmaa-Klaar is Ambassador for Cyber Diplomacy and Director General for the Cyber Diplomacy Department at the Estonian Ministry of Foreign Affairs. She was the expert appointed to the 2019-2021 UNGGE by the Estonian government.

a common interest in achieving agreement. The other elements playing a role in the successful outcome of negotiations are comprised of proficiency of the chairs, expectations by the group members, regional dynamics, effective backchanneling efforts, and increasing professionalization of GGE members.

The UN discussions on cyber norms are nearly as old as the World Wide Web itself.[1] The central role of technology in the political-military context became evident in the beginning of the 1990s when the United States gained a dominant position in terms of technological advancement, also manifested in its military supremacy. A short Gulf War in 1991 demonstrated that the use of high-technology conventional weapons has created clear advantages for the U.S. led coalition forces.[2]

Recognizing the U.S. dominance in information and communications technology (ICT), the Russian Federation first proposed to discuss the ICT issues in the context of international security in the UN as early as 1998. After several attempts to use different UN venues to start discussions, it was decided that the best way forward was to create a Group of Governmental Experts (GGE) under the Disarmament Committee. The United Nations General Assembly uses GGEs as a common tool by which to examine emerging security topics relevant to international security, such as transparency and confidence-building measures in outer space activities, or the use of lethal autonomous weapons systems. The Russian Federation proposed a UNGA resolution in 2002 that called for the creation of the GGE to study threats and possible cooperative measures in cyberspace.[3]

It was not until 2007 that the broader public discovered that the cyber domain became a source of strategic risk that could destabilize countries and create large-scale political and economic havoc.

The first GGE on cyber issues gathered under the auspices of the UN Disarmament Committee in 2004–2005. This first attempt did not result in the consensus report for several reasons, among which were the unwillingness of the UN Security Council permanent members to agree on the direction of the report, and the lack of broader international interest toward cyber stability issues at that time.

According to several different accounts on the history of cyber conflict, the period before 2007 featured low levels of cyber threat awareness among top decision-makers, diplomats, and military leaders. Serious cyber intrusions into military systems and cyber intelligence operations rarely made any headlines, but stayed in the confines of national security-related confidential files.[4] During this period, cybersecurity was generally seen as a technical issue, a task for information security management teams and IT departments both in the public and the private sectors.

It was not until 2007 that the broader public discovered that the cyber domain became a source of strategic risk that could destabilize countries and create large-scale political and economic havoc. During the ”bronze soldier monument” events in Estonia, the country experienced a Russian hybrid campaign aided by the first publicly known large-scale cyber operation that resulted in many online targets in Estonia being subjected to a state of digital siege. In retrospect, the Estonian events served as a wake-up call that demonstrated how cyberattacks and hybrid operations can be used in a geostrategic context for advancing foreign policy goals.

It should be noted that in 2007 Estonia was already one of Europe’s most wired countries, with many private and public sector services available online. It had, for instance, introduced a na

tion-wide digital authentication system used by the majority of the population. Several waves of cyberattacks, most of them in the form of DDoS (Distributed Denial of Service) attacks, targeted media outlets, online banking, and governmental websites.[5] During the three weeks of cyber siege, the Estonians were forced at some point to limit their connectivity to the World Wide Web in order for the Internet services inside the country to continue, and only locals could still carry out essential transactions online as they were accustomed to doing. Targets of the DDoS attacks were mostly websites, and the cyber operations stayed away from the electricity, transport, industrial control systems, and military networks. Except for online banking services and governmental websites, the botnets that were employed did not target civilian critical infrastructure, i.e., malicious cyber activities clearly stayed below the threshold of an armed attack.

Although this hybrid campaign originating from the relocation of a Soviet WWII monument had many elements, the cyberattacks received much wider international media attention compared to organized riots in the streets and the physical blockading of the Estonian Embassy in Moscow or the closing of the land border to Russia to transit flows. The 2007 Estonian cyber siege is widely known as the first significant cyber event, and has catapulted the formerly technical cyber issues into the limelight. Never before had large-scale cyberattacks been used to "punish" a country for activities that run against the foreign policy interests of another country. This event put cybersecurity onto the map of foreign and security policy senior decision-makers, and marked a starting point for cyber issues becoming increasingly mainstreamed to a more strategic level, both nationally and internationally.

In 2006–2008, several notable cyber incidents took place against the U.S. and European governmental networks, as well as private-sector targets, especially the banking and oil sectors.[6] Reporting on cyber incidents grew, and the policymakers became aware of the need to find commonly accepted rules that would set boundaries of state activities in cyberspace. A new kind of visible cyber operation was conducted by Russia during the short war between Russia and Georgia in 2008. Although technologically not too sophisticated, but nonetheless effective, the DDoS and defacement attacks against Georgian media outlets and governmental websites were taken out of the same playbook as attacks on Estonia a year earlier.[7] The operation against Georgia was in support of the overall objective to cut off strategic communication capabilities during the first days of conflict and discredit the country internationally. Again, these cyberattacks became widely known and published in the world media.

After the events in Georgia in 2008, cyber threats undeniably became security and foreign policy concerns, and policymakers started to look for venues where the question of setting acceptable state behavior in cyberspace could be raised. Interestingly, in 2006 a new UNGA resolution had been proposed by the Russian Federation to create a new GGE in 2009.[8] Ironically, the UN member states' growing support of the Russian annual UNGA resolutions on developments in the field of ICTs in the context of international security was facilitated by the number of significant attacks against their networks.

Following these events, the GGE process started to gain in maturity. The second UN GGE started in 2009 with the mission "...to continue to study existing and potential threats in the sphere of information security and possible cooperative measures to address them."[9] The process of setting boundaries for state behavior in cyberspace now truly began against the background of a growing number of significant cyber incidents.

The 2010 GGE report recognizes that cyber threats "...are among the most serious challenges of the twenty-first century...their effects carry significant risk for public safety, the security of nations, and the stability of the globally linked international community..."[10] The 2009–2010 GGE negotiations led to a recommendation that further dialogue among states is necessary to reduce risk and protect critical infrastructure. The recommendations sections also called for "confidence building, stability, and risk reduction measures to address the implications of state use of ICTs."[11] The 2010 report is a short one, consisting of threats, cooperation measures, and recommendations. Allegedly, there was a longer report prepared but discarded at the last minute. Nevertheless, consensus was found to continue discussions and the report has paved the way to more fruitful GGEs in the future.

Although the process was regarded as very important by a handful of cyber connoisseurs in the foreign ministries and nascent cyber forces, the larger public policy and national security community were still generally unaware of this group gathering "somewhere in the UN basement," as one cyber expert participating in discussions called it. More than the report itself, the 2009–2010 process was an important vehicle for forming a nascent international cyber community coalescing around this issue, and it defined a group of nations that were dedicating time and resources to figuring out international policy for regulating state behavior in cyberspace. It also created a precedent for cyber issues to be discussed in the UN First Committee agenda as part of international security, taking it further from the perception that cybersecurity is limited to a dusty server room. Some participants also characterized these early days as creating "positive tension" between technical cyber geeks and non-technical policy wonks, helping to show that the wonks also had something valuable to offer to this field.

The GGE of 2012–2013 took this one step further and produced a very solid and coherent report. The document references all four major elements that will later be declared as a framework for responsible state behavior in cyberspace.[12] These include the application of existing international law, voluntary non-binding peacetime norms of responsible state behavior, confidence and cooperation measures, and capacity-building measures. The report also introduced a chapter on threats, risks and vulnerabilities, and mentioned the role of regional organizations in advancing cyber cooperation.

The 2013 report is best known for its strong affirmation of the international law obligations to state behavior in cyberspace. It claims that international law, and in particular the UN Charter as well as the Universal Declaration of Human Rights, apply in cyberspace. The report goes further in establishing that "the application of norms derived from existing international law relevant to the use of ICTs by states is an essential measure to reduce risks to international peace, security, and stability."[13] Paragraph 23 of this report captures three key obligations for state behavior that are still very relevant: "States must meet their international obligations regarding internationally wrongful acts attributable to them. States must not use proxies to commit internationally wrongful acts. States should seek to ensure that their territories are not used by non-state actors for unlawful use of ICTs."[14]

The question of the applicability of international law has been an especially controversial one since the start of the GGE discussions. The Western likeminded governments have always stressed the applicability of the existing international law, which needs to be applied in the cyber context. The key obligations for state behavior in peacetime, mentioned in the previous paragraph, are derived from the existing international law. The UN Charter and International Humanitarian Law provide sufficient guidance for state behavior in times of conflict, both in jus ad bello and jus in bellum. It was

expected that states develop legal norms codified by these existing bodies of law, and that this would have a tremendous stabilizing effect on cyberspace.

However, the Russian Federation proposed a Code of Conduct on Information Security as early as 1998 that calls for a special UN instrument to include different measures that would bolster information security.[15] The same proposal with some updates was repeated by China and Russia in 2011, and again by the members of the Shanghai Cooperation Organisation in 2015, this time also including a recommendation to change the current Internet model that would give governments an upper hand on Internet governance instead of the multistakeholder community.[16] As the Western governments feared the Code would facilitate further content control, changes in Internet governance, and would mostly be used for legitimizing censorship by authoritarian regimes,[17] they have strongly opposed an emergence of a legally binding instrument during the UN First Committee discussions. The conversation around international law has been a central preoccupation of all GGEs after 2013, and was one of the root causes for the failure to find consensus in 2017.

In retrospect, the 2013 GGE report paved the way for a more advanced 2015 report that still remains a gold standard for setting boundaries of state behavior in cyberspace through its eleven non-binding voluntary peacetime norms for responsible state behavior. When these norms were negotiated in 2015, the participants in the room could not have known that their work would establish a central framework by which to regulate state cyber behavior for the next decade. These norms include additional commitments by states to cooperate, assist, and consult in cases of cyber incidents, to refrain from activities that can affect critical infrastructure, and to abide by a specific norm to protect computer incident response teams, which should not be attacked and should themselves not engage in malicious cyber activities. It also mentions attribution, supply chain and vulnerability disclosure as new elements compared to the 2013 report. In addition, the report makes substantial recommendations on confidence and capacity-building measures.

Among other areas of professionalization of the GGE discussions, a more nuanced separate section on applying international law was added to the 2015 report. It repeats some of the obligations mentioned in 2013, but also mentions new elements, such as the principles of humanity, necessity, proportionality, and distinction from the International Humanitarian Law (IHL). The IHL itself is not mentioned due to an argument by one GGE expert that if the jus in bello body of law will be cited it legitimizes the use of cyberspace for military purposes. A majority of the observers does not see a direct link in how recognizing the IHL applicability can militarize cyberspace, but this has been a long-standing argument by experts from China and has complicated international law discussions in many GGEs.

After the 2015 consensus was achieved, it left everyone a little disappointed, but was still (or because of that) praised as a major step forward in retrospect. Negotiations in 2016 started with an understanding that the new report should add recommendations on how to implement norms of responsible state behavior. However, the 2016–2017 GGE process did not bring consensus for several reasons, among which was disagreement on international law. One of the central elements for the failure was a worsening geostrategic relationship between major powers due to the Russian interference in the U.S. presidential elections in 2016.

The collapse of the 2016–2017 GGE created a collective wound, especially since the number and sophistication of cyber operations had grown exponentially, leaving states to wonder how they can use international mechanisms to better protect themselves and to respond more effectively to

malicious cyber activities. Although the regional organizations (OSCE, ARF, OAS, etc.), the Global Commission on the Stability of Cyberspace (GCSC), and other multistakeholder fora were attempted to fill the cyber norm-creation vacuum, without the formal UN umbrella it did not have the same diplomatic weight, albeit they all provided a very valuable addition to the global cyber debate.

In the Fall of 2018, the international cyber community confronted the UNGA73 season with new enthusiasm to re-establish the cyber norms debate in the First Committee. Despite the newly found optimism, it was quite clear that the drama that led to the failure in 2017 was still casting its shadows on UN cyber negotiations. There were two cyber resolutions on the table in 2018, one by the U.S. and one by Russia. The U.S. resolution was calling for the creation of the new GGE to provide an additional understanding of how the agreed norms could be implemented, and called for issuing a separate annex with national contributions on how the international law applies in cyberspace.[18]

In this resolution, the controversial issue of international law was parked outside the report with the hope that it would make consensus-building easier later. As a post-factum note, the annex on international law was still one of the last critical open questions until the very end of negotiations, before reaching consensus during the most recent GGE in 2021.

While the U.S.put forward a resolution for a new GGE, Russia had a new initiative in mind. The Russian resolution contained a mix of different old and new paragraphs, some not too much related to the cyber context. But the text called for the creation of the inclusive Open Ended Working Group (OEWG) that created a possibility to have a seat at the cyber table for all UN states—a prospect that many found attractive.[19] Further, unlike the GGE, the OEWG promised to at least "consult" non-state experts—although this factor was heavily diluted during implementation.

The idea of the new OEWG was not overly popular among the liberal democratic like-minded nations in the beginning, as it raised again the questions of the actual motives for the creation of the new group, and whether the OEWG would become a battlefield between two different visions of the future of cyberspace, democratic and autocratic. The fears of introduction of a new legal instrument re-emerged as did memories of other difficult discussions from previous GGEs. The tension was somewhat eased after careful selection of chairs to both processes, who were experienced Brazilian and Swiss diplomats. With the choice of neutral chairs, hope was restored that objectivity would prevail in the First Committee cyber discussions. To manage the two parallel groups, UNODA was in a difficult position to come up with a schedule of OEWG and GGE sessions that would facilitate a coordinated approach. An overall concern was how to create complementarity between the two groups, instead of competing processes.

In September 2019, all nations participating in GGE 2019–2021 entered the first substantive OEWG discussion in New York with well-prepared dossiers, ready to stand up for the achievements of previous GGEs and, if needed, eager to defend the added value of the current GGE. In fact, already during the first days of the OEWG session, most of the newcomers at the table from the wider UN membership repeated the mantra: "We are not starting here from scratch, but will build this OEWG process on already achieved consensus by previous GGEs." It became evident that the important four tenets cemented by previous GGEs had become a clear guiding framework for all nations, who were just happy to have a seat at the UN cyber table finally, and were not particularly keen to be regarded as puppets of the OEWG originator. The European Union member states also brought the EU jargon of commonly agreed legal basis, "acquis," to the UN context to signify the consensus by previous GGEs.

After the first meeting in September 2019, the initial weariness about the formation of the OEWG gave way to cautious hope on the possibility to have two complementary processes that serve slightly different objectives. The GGE was expected to create an additional layer of understanding of norms of responsible state behavior and would be driven by a relatively small group, whereas the OEWG would become an inclusive awareness-raising and socializing body on the existing consensus on international law, norms of responsible state behavior, confidence-building measures, and capacity building.

It became evident that the important four tenets cemented by previous GGEs had become a clear guiding framework for all nations, who were just happy to have a seat at the UN cyber table finally.

The first GGE session in New York in December 2019 was a friendly gathering of experts, old and new, who were almost exclusively senior-level diplomats or civil servants with important cyber policy roles. When choosing GGE members, the UN Secretary General had tasked UNODA to seek, in addition to regional balance, also a gender balance. The gender balance was certainly more equal in this GGE round, and served as an important element that contributed to the success of the group as observed by one GGE expert.

The first two GGE meetings were running relatively smoothly until the second session in Geneva in 2020, after which the pandemic struck and changed everything. Both the GGE and OEWG moved to virtual meeting rooms with an uncertain prospective of their outcomes.

Due to difficulty in managing meetings in a way that experts from all time zones could attend during business hours, the meetings took place during European, African, Middle Eastern, and American working hours. Many of the Asia-Pacific GGE experts had to work in the middle of night, and endure the whole week with little sleep as they also had to fulfil their responsibilities during the working day. Despite all these complexities, the sessions were very professional and substantive, allowing enough face time for the experts to react to other experts, and room for the chair to maneuver through the difficult questions. Participants applauded the always calm and diplomatic Brazilian chair, Ambassador Guilherme Patriota, who was stuck in Mumbay as the Brazilian Consul General during the whole pandemic and managed to keep the online sessions of GGEs running.

Although the pandemic brought major disruptions to GGE experts' routine lives and strained the work schedules with too many online events, it also allowed for more sessions than usual. The resulting report of the 2019–2021 GGE could be characterized as a rare victory of multilateral diplomacy where all parties to negotiations felt that they had won something. For the Western nations, important mentions of international law were included in the report as well as substantial paragraphs on attribution and explanations on critical infrastructure protection norms. The attached compendium on international law has created a solid collection of national views on this central issue. China walked away with the desired text on supply chain, and Russia was able to get in the sentence on new OEWG. Developing nations were also satisfied with the report on further cooperation, consultations, and capacity-building points.

In order to analyze what factors aided the process of building consensus in 2019–2021, the leading drafter in the GGE secretariat, Camino Kavanagh from the UNIDIR support team, has attributed the success to many favorable factors that were mutually reinforcing, especially the work done by the chairs and the secretariat that allowed for coordination of the draft reports, as well as timing of the events.[20]

It should be noted that many saw the parallel processes as two sides of the same coin. This "hostage situation" was nerve-racking for all states who were looking forward to having clear guidance by the United Nations and who wanted to see results in both processes.

The Australian GGE expert, Johanna Weaver, praised the high quality of work by the secretariat and chairs, and observed the overall desire by nations to achieve consensus recommendations as a result of the first inclusive UN cyber format, which could then be replicated in a smaller GGE group in a more detailed manner: "The OEWG was a success because at the last meeting we had an excellent draft on the table and 'middle-ground' countries had repeatedly and publicly underscored that no-outcome was not an option. This helped apply pressure to bring the 'great powers' to the table; no great (or less great) power wanted to be the one to cop the blame for getting in the way of a defensibly good report that everyone wanted."[21]

On reaching the consensus in the 2021 GGE, she observed: "The final GGE meeting occurred after the inaugural OEWG concluded, but just days before the organizational session of the new OEWG. This, combined with dynamics that flowed from other unrelated but concurrent UN fora, as well as geopolitical goings-on external to the UN, all aligned to create a climate where consensus was within reach. We had another excellent draft on the table. In the final hours, it would be wrong to say that all interests aligned, but everyone needed something, and we were able to find a way to give each what they needed without impinging on others redlines."[22]

In successful international negotiations, there are usually many coinciding elements that have come together in certain points of time and produced a desired outcome. This was also the case with all successful GGE outcomes, where internal GGE group dynamics and other factors coincided with a broader enabling strategic environment.

The 2009–2010 process was regarded as the first successful GGE that allowed the work to continue on shaping international cyber norms and created the community of nations interested in the topic. However, it is also very important to note that the new U.S. administration had been inaugurated in 2009, which changed the direction of the U.S. cyber policy that facilitated reaching the GGE goals. President Obama had issued its Cyberspace Policy Review in May 2009 with recommendations on both national and international activities.[23] This gave the U.S. diplomats a green light with which to engage in the UN discussions.

During the 2012–2013 GGE negotiations, President Obama and President Putin agreed to establish a new working group within the U.S.–Russia Bilateral Presidential Commission as a part of the cybersecurity confidence-building measures between the U.S. and Russia. Already in early 2011, the U.S. and Russia had started regular discussions on cyber confidence-building measures to avoid accidential escalation, and agreed to establish a U.S.–Russia cyber hotline similar to the nuclear hotline from the Cold War days.[24] This has also faciliated the adoption of the first set of cybersecurity confidence-building measures in the OSCE in 2013.

As a broader enabling factor in 2015, the final GGE session in July preceded the President Obama meeting with Xi Jinping in September 2015, where the bilateral agreement was reached, to not "... knowingly support the cyber-enabled theft of intellectual property, including trade secrets or other confidential business information for commercial advantage."[25]

In 2021, several elements in the ongoing UN First Committee cyber debates could be attributed to positive GGE outcomes, but there was also an overarching political motive for working toward

consensus before the U.S.–Russia Summit that was announced to be taking place in June in Geneva. The announcement on the Summit date came out two days before the GGE final report was concluded on the 28th of May. In a way, the ongoing cyber GGE negotiations became but one piece in a larger geopolitical puzzle that was put together before the summit.

The first U.S. cyber envoy, Christopher Painter, assessed that a wider geopolitical context always played an important role in contributing success to different GGEs:

> "The GGE, like any other development in cyberspace, is tied to the larger geopolitical environment and political will. When geopolitical tensions between Russia and the United States are relatively low and stable, as was the case in 2013, agreement and consensus in the GGE is more likely. When they are very high , as in 2017 because of Russian election interference and other malicious activity, consensus and agreement are unlikely. Yet, this doesn't tell the whole story. Even when larger geopolitical tensions are high between the two countries, they can and have still reached agreement if it is in both of their strategic interests and there is political will. A significant consensus was reached in 2015 despite Russia's invasion of the Ukraine and the consequent suspension of the high-level US–Russia cyber dialogue because both countries saw value in the articulation of a normative framework for cyberspace and the continuation of the GGE. Agreement was reached again in 2021 despite continued poor relations between the US and Russia on both cyber and non-cyber issues. However, as cyber issues continue to be elevated as a national security issue and integrated into broader national security and diplomatic priorities, it is likely that the success or failure of cyber negotiations, like any other negotiations, will increasingly be dependent on the overall relationship between the countries who are major players."[26]

It is essential to note that, in parallel to GGEs taking place in the UN, a number of regional organizations started discussions on cyber confidence-building measures, norms, international law, and capacity building, further mainstreaming the four elements in the GGE reports as a normative basis for state behavior. The OSCE adopted two sets of cyber security confidence-building measures in 2013 and 2016, and continues to implement these measures through its cybersecurity working group.[27] The ASEAN Regional Forum has discussed cyber confidence-building questions since 2012,[28] and the ASEAN ministerial conference on cybersecurity has endorsed the eleven norms of responsible state behavior from the 2015 GGE report.[29] The Organisation of American States has an active Cyber Security Programme facilitating the exchange of best practices, training, and education among all its members, as well as implementation of capacity-building projects.[30] The European Union has mainstreamed the issue of cyber diplomacy into its policy proceedings since the 2013 EU first Cyber Security Strategy.[31] All these regional initiatives have further raised awareness of GGE agreements on cyber norms, confidence-building measures, and international law applicable in the cyber domain. They have also helped to increase global interest toward ongoing UN cyber negotiations, and have created additional expectations for each GGE to progress with discussions in order to provide better guidance for state behavior.

In parallel to GGEs taking place in the UN, a number of regional organizations started discussions on cyber confidence-building measures, norms, international law, and capacity building, further mainstreaming the four elements in the GGE reports as a normative basis for state behavior.

One of the central elements contributing to the success of different GGEs was also the composition of the group, which has determined the discussion dynamics. In earlier years, the composition of the GGEs was a mix of technical cyber experts, military officers, academics, and diplomats. The first GGEs also included a few academics and technical experts, but each successive GGE had more diplomats with international security and arms control backgrounds involved. The gradual professionalization of the "cyber diplomat tradecraft" was noticeable also in the quality and substance of the negotiations. By the 2019–2021 GGE, there were already diplomats with specific cyber expertise who emerged in many MFAs, which made the difference in the quality of discussions. As one of the experts recalls: "It is not so much that there were increasing numbers of diplomats in the room; rather, it was that there were increasing number of diplomats that specialized in cyber policy in the room. There are nuanced differences in cyber policy and arms control. Some skills are transferable, but subject matter expertise—of cyber as a strategic foreign policy issue—is what brought depth to the discussions."[32]

Naturally, there were also principals among the experts who provided steadiness and historical memory for the group. For the cyber diplomats' community, it is quite well known that the continuity of discussions for rules of the road in cyberspace was essentially up to two skillful diplomats, Michele Markoff from the United States and Andrey Krutskyh from Russia. They had been working together already during the Cold War on several disarmament issues, and were founding members of cyber GGEs. The dynamic between the two senior and experienced cyber experts from two superpowers in the room often defined the atmosphere of negotiations. Without the long-standing relationship between them, it would be hard to imagine the GGEs as we know them.

The chairs of each GGE reiteration also played a major role in setting the tone for each group. The 2009–2010 GGE was chaired by Andrey Krutskyh from the Russian Federation, who was the initiator of the whole UN First Committee cyber discussion. In 2012–2013, the chair was a senior Australian diplomat, Deborah Stokes, who was praised for her ability and skills to build consensus. In 2014–2015, the Brazilian chair, Carlos Perez, was known for effective backchanneling between the experts and for solving complex negotiations with personal diplomacy efforts. In 2016–2017, the chair was one of the first European cyber diplomats, Karsten Geier from Germany, who had a high degree of subject matter expertise and tried everything in his power to reach consensus despite the political climate. In 2019, expectations were very high when Ambassador Guilherme de Aguiar Patriota took over the GGE chairmanship. He had outstanding experience in chairing a number of GGEs before, and this was visible in the room where he could skillfully steer discussions, and also virtually, even when some delegates proved to be difficult from time to time.

In addition, there were also UNODA and UNIDIR team members who provided the secretariat for each GGE as well as OEWG, and created consistency between different reiterations of groups. Kerstin Vignard, James Lewis, Camino Kavanagh, and Gillian Goh were key players behind the scenes who brought difficult drafting processes to a victorious end.

It would be unfair not to mention a significant negotiator who was instrumental in bridging the OEWG and GGE discussions to achieve consensus in the final rounds of March to May of 2021. The Australian GGE expert, Johanna Weaver, worked magic in New York in the spring of 2021 and facilitated sometimes tough negotiations between UN member states in the final stages of the two working groups. During the ongoing pandemic, with limited international travel, she was volunteering to establish a presence in New York for three months and proved especially efficient in arbitraging final GGE disputes between key players.

Looking at the composition of the each GGE, there were many other outstanding cyber experts and diplomats, all of whom played key roles in the process and provided valuable contributions to each GGE.[33] As the cyber issues gained more relevance to foreign and security policy, the group grew from the initial fifteen members to twenty-five by 2021. The UN Security Council's permanent five members were always present in the group, leaving few seats left over, for which countries were competing intensely each time a new GGE emerged. Picking the members of the group was always a complex process, where, in addition to regional balance, the cyber expertise and negotiating experience of each expert was evaluated by UNODA.

As the analysis above demonstrates, each different GGE took place in a specific geostrategic context and was influenced by many simultaneous dynamics. It requires further in-depth analysis to determine what exactly brought success or failure to each GGE process, due to the complexity of international multilateral negotiations as there were many influential factors behind the scenes that are rarely known to the wider public. The history of cyber GGEs certainly deserves a longer account that would also include the memoirs of key players, and more substantive analysis than the short format of this article allows. Michele Markoff suggests that successful outcomes were brought by "common interest in preventing conflict and an atmosphere conducive to political will and collaboration."[34]

The conclusion can be made that the GGEs achieved consensus when taking place during a favorable geopolitical context, where tensions between the leading powers were relatively low or there was otherwise a common interest in achieving agreement.

In very general terms, the conclusion can be made that the GGEs achieved consensus when taking place during a favorable geopolitical context, where tensions between the leading powers were relatively low or there was otherwise a common interest in achieving agreement. Other elements playing a role in the successful outcome of negotiations are comprised of proficiency of the chairs, expectations by the group members, regional dynamics, effective backchanneling efforts, and increasing professionalization of GGE members.

Conclusion

With six GGEs from 2004 to 2021, a solid foundation is built for more predictable state behavior. Four elements discussed above, including the application of existing international law, voluntary non-binding peacetime norms, confidence building, and capacity-building measures form a normative framework for responsible state behavior. Different iterations of GGEs that have developed norms and guidance on norm implementation as well as the OEWG recommendations have brought the international cyber community to a good place by the end of 2021. Now the challenge of implementation of these recommendations lies ahead. The next milestone for the First Committee cyber discussions will be a first substantive session of the new Russian-proposed OEWG in December 2021. There is also a proposal for the Programme of Action presented by France and Egypt and co-sponsored by more than fifty countries with the ambition to steer the operationalization of the recommendations. It is hard to predict which process will be more efficient in the long run, but it is quite clear that there are many UN member states that still need to build expertise on how to implement cyber norms and apply international law.

Endnotes

1 This is using the definition of the World Wide Web that has arisen with the widespread introduction of websites and web browsers after 1994/1995.

2 Gene Rochlin and Chris Demchak, "The Gulf war: technological and organizational implications," Survival 33, no. 3 (May/June 1991): pp 260–273, https://www.tandfonline.com/doi/abs/10.1080/00396339108442594.

3 United Nations General Assembly, "Resolution adopted by the General Assembly on Developments in the Field of Information and Telecommunications in the Context of International Security" A/RES/56/19, United Nations, January 7, 2002. https://digitallibrary.un.org/record/453522?ln=en#record-files-collapse-header

4 Jason Healey, "A Brief History of US Cyber Conflict" in Healey ed. A Fierce Domain: Conflict in Cyberspace, 1986 to 2012 (Cyber Conflict Studies Associated Publication, in Partnership with the Atlantic Council, 2013): pp. 15–40.

5 Andreas Schmidt "The Estonian Cyberattacks," in Healey ed. A Fierce Domain: Conflict in Cyberspace, 1986 to 2012 (Cyber Conflict Studies Associated Publication, in Partnership with the Atlantic Council, 2013).

6 "Significant cyber incidents since 2006," Center for Strategic and International Studies, accessed 24.10.2021, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

7 "Georgia-Russia Conflict 2008," CCDCOE, accessed 24.10.2021, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

8 United Nations General Assembly, "Resolution adopted by the General Assembly on 6 December 2006 on Developments in the Field of Information and Telecommunications in the Context of International Security," A/RES/61/54, United Nations, December 19, 2006. https://undocs.org/A/RES/61/54

9 Ibid.

10 United Nations General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," A/68/98, United Nation, June 24, 2013. https://undocs.org/A/68/98

11 Ibid.

12 Ibid.

13 Ibid.

14 Ibid.

15 For further analysis on how the Russian and Western approaches differ on cybersecurity, see Alexander Klimburg, The Darkening Web: the War for Cyberspace, (New York: Penguin Books: NY, 2017): pp.117–129.

16 United Nations General Assembly, "Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgystan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General", A/69/723, United Nations, January 13, 2015. https://undocs.org/A/69/723

17 John Markoff and Andrew Kramer, "U.S. and Russia Differ on a Treaty for Cyberspace", New York Times, June 27, 2009, https://www.nytimes.com/2009/06/28/world/28cyber.html

18 United Nations General Assembly, "Resolution adopted by the General Assembly on 22 December 2018 on Advancing responsible State behaviour in cyberspace in the context of international security," A/RES/73/266, United Nations, January 2, 2019. https://undocs.org/A/RES/73/266

19 United Nations General Assembly, "Resolution adopted by the General Assembly on 5 December 2018 on Developments in the field of information and telecommunications in the con

text of international security", A/RES/73/27, United Nations, December 11, 2018. https://undocs.org/en/A/RES/73/27

20 "The positive outcome of the OEWG and GGE was due to a combination of factors. These include the commitment of UN member states and experts; the continuity provided by the common secretariat which supported both chairs and processes; diplomatic skills and coordinated approach to both processes by two chairs; the engagement of multiple actors in the processes enabled by both resolutions and their provisions for consultations; and broader diplomatic developments which contributed to making the environment more conducive to positive outcomes." Interview with Camino Kavanagh, a member of UN GGE and OEWG secretariat on 21 September 2021.

21 Interview with Johanna Weaver, former Head of Australian Delegation to the UN OEWG and GGE on 21 October 2021.

22 Ibid.

23 "The Comprehensive National Cybersecurity Initiative," White House President Barack Obama, accessed on October 24, 2021, https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative

24 Timothy Farnsworth, "US, Russia to Discuss Cyber Hotline," Arms Control Association, accessed on October 24, 2021, https://www.armscontrol.org/act/2012-05/us-russia-discuss-cyber-hotline

25 "Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference", White House President Barack Obama, September 25, 2015. https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint

26 Online linterview with Christopher Painter, the former U.S. State Department Cyber Coordinator on 26 October 2021.

27 See more detailed information on the OSCE cyber activities at "Cyber/ICT Security", OSCE, https://www.osce.org/secretariat/cyber-ict-security

28 "Annex 11. ASEAN Regional Forum Experts and Eminent Persons (ARF/EEP) Recommendations for ARF Initiatives on Promoting Cyber Security," ASEAN Regional Forum, March 6, 2018, at https://aseanregionalforum.asean.org/wp-content/uploads/2019/01/ANNEX-11-ARF-EEP-FINAL-REPORT.pdf

29 Elina Noor, "ASEAN Takes a Bold Cybersecurity Step," The Diplomat, October 4, 2018, https://thediplomat.com/2018/10/asean-takes-a-bold-cybersecurity-step/ .

30 "Cybersecurity program", OAS, https://www.oas.org/en/sms/cicte/prog-cybersecurity.asp

31 European Commission, "JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", European Union, February 7, 2013. https://op.europa.eu/en/publication-detail/-/publication/e8ab3970-f86e-41a6-8666-33e94614dcf2/language-en

32 Interview with Johanna Weaver, former Head of Australian Delegation to the UN OEWG and GGE on 21 October 2021.

33 The composition of each GGE is described in reports and can be accessed at "Group of Governmental Experts," United Nations, https://www.un.org/disarmament/group-of-governmental-experts/

34 Online linterview with Michele Markoff, the U.S. State Department Acting Coordinator for Cyber Affairs on 18 November 2021.

About the Author

Heli Tiirmaa-Klaar is Ambassador for Cyber Diplomacy and Director General for the Cyber Diplomacy Department at the Estonian Ministry of Foreign Affairs. Up to Fall 2018, she was working as a Head of Cyber Policy Coordination at the European External Action Service where she steered and coordinated EU external relations on cyber issues since 2012. She set up EU strategic cyber dialogues with the US, India, Brazil, Japan, South Korea as well as other international organisations. She also kicked off EU global cyber capacity building programs and steered the development of the EU Cyber Diplomacy Toolbox to bolster EU response to malicious cyber activities. In 2011, she was assigned to the NATO International Staff to prepare the NATO Cyber Defence Policy.

She has been working on cyber security since 2007 when she led the development of the Estonian Cyber Security Strategy. In 2008-2010 she coordinated the implementation of the Estonian strategy, managed the National Cyber Security Council and led the establishment of Estonia's national cyber resilience structures as well as public-private partnerships for cyber security. In her earlier career, she held various managerial positions at the Estonian Ministry of Defence and the Tallinn University. She was a Fulbright Scholar at the George Washington University and has published in several academic journals throughout her career.

Cyberstability Paper Series
New Conditions and Constellations in Cyber

From Confrontation to Consensus: Taking Stock of the OEWG Process

Ambassador Jürg Lauber
Chair of the first UN Open-ended Working Group on developments in the field of information and telecommunications in the context of international security from 2019 until 2021.

Lukas Eberli
Second Secretary for Cybersecurity at the Permanent Mission of Switzerland to the United Nations and other international organizations in Geneva

From Confrontation to Consensus: Taking Stock of the OEWG Process

Ambassador Jürg Lauber | Chair of the first UN Open-ended Working Group on developments in the field of information and telecommunications in the context of international security from 2019 until 2021.

Lukas Eberli | Second Secretary for Cybersecurity at the Permanent Mission of Switzerland to the United Nations and other international organizations in Geneva

On 28 April 2021, the General Assembly of the United Nations ("UNGA") endorsed[1] the report of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security ("OEWG"). The UNGA's decision brought to a close a process that had been initiated by the General Assembly's First Committee in the fall of 2018, and whose successful outcome came as a surprise to many. The OEWG report provides a very strong reconfirmation of the existing normative framework with regard to cybersecurity, while it adds a number of essential new elements and offers a rich compendium of ideas and proposals for future deliberations on the same issue. The first-ever UN Open-ended Working Group on this issue brought cybersecurity into the multilateral mainstream, with the UN General Assembly at its center. It made a strong case for universal participation in discussions of a topic that is vital to all nations.

I had the privilege of serving as the Chair of this first OEWG. In this article, I will mainly describe the OEWG process from the Chair's perspective and try to explain how and why we were able to pull back from confrontation and reestablish consensus. I will also give a brief and personal assessment of the outcome and, finally, share a few thoughts about the way forward.

Ambassador Jürg Lauber currently serves as the Permanent Representative of Switzerland to the United Nations Office and the other international organizations in Geneva. He served as the Chair of the first UN Open-ended Working Group on developments in the field of information and telecommunications in the context of international security from 2019 until 2021.

Lukas Eberli served as the Adviser to Ambassador Jürg Lauber's Chairmanship of the UN OEWG. Currently, he Second Secretary for Cybersecurity at the Permanent Mission of Switzerland to the United Nations and the other international organisations in Geneva.

When the General Assembly of the United Nations established the OEWG in December 2018 by Resolution 73/27[2], this particular format—enabling the participation of all Member States and observers of the United Nations—was a first for cybersecurity. The issue, however, was far from new to the United Nations. It had been on the agenda since 1998 and was primarily dealt with by five subsequent Groups of Governmental Experts on Advancing responsible State behavior in cyberspace in the context of international security ("GGE"). In addition, there had been annual reports by the Secretary-General to the General Assembly with the views submitted by UN Member States on the issue. By 2015, the GGE format had produced a sophisticated normative framework (often referred to as the "acquis"), essentially comprising three pillars: 1) Eleven non-binding norms of responsible state behavior in cyberspace, 2) A common understanding of the applicability of existing international law, and 3) Confidence-building measures. No progress was achieved in the following years, and the inability of UN Member States to find consensus in their deliberations on the subject of cybersecurity was starting to threaten the integrity of the 2015 acquis. Indeed, the Russian draft resolution to establish the OEWG was opposed by a significant number of delegations[3] for its particular interpretation of earlier agreed-upon voluntary non-binding norms.

According to its mandate as contained in Operational Paragraph 5 of UNGA Res 73/27, the OEWG was to deliberate and report on six items:

- First, Existing and Potential Threats;
- Second, Rules, Norms and Principles;
- Third, International Law;
- Fourth, Confidence-Building Measures;
- Fifth, Capacity-building; and
- Sixth, Regular Institutional Dialogue.

Importantly, the OEWG was required to adopt its report by consensus. Finally, the mandate offered a first, if cautious, opening toward non-governmental stakeholders ("namely, business, non-governmental organizations, and academia"; hereafter generally referred to as "stakeholders").

Based on draft resolution 73/266 of 22 December 2018[4], submitted by the United States, the General Assembly of the United Nations also established another, sixth GGE with a very similar mandate and twenty-five members. This led to the unusual situation of having two UN bodies dealing in parallel with almost the exact same issues.

For the OEWG Chair, the central task was to work with the Group in such a way as to soften the fronts that had hardened since 2015, and ultimately present a document that would be acceptable to all States as well as deliver added value for as many as possible. The GGEs of the past had comprised up to twenty-five members. In the OEWG, all 193 Member States of the United Nations would have a say. The much higher number and diversity of the OEWG made the challenge to find consensus all the more daunting, but it also offered the promise of new dynamics emanating from groups and individual Member States that had little or no representation in previous GGEs. This is, e.g., reflected in the very substantive chapter on cybersecurity capacity-building in the OEWG's report, an issue that had never attracted this much attention in past GGEs. With this in mind, I based my strategy for the negotiation process on the principles of inclusiveness, transparency, and cautious ambition. For instance, my team and I made great efforts to reach out to the various regional and other groups of Member States as well as to the so-called (non-governmental) stakeholders. We wanted to ensure that as many of them as possible would participate in the deliberations, thus underpinning the legitimacy of the process and its possible outcome. We also made sure that all

interested parties had equal access to information about the Chair's intentions with regard to the process and the draft report.

According to the mandate of the OEWG and the original work plan, we had scheduled three substantive sessions, one intersessional stakeholder meeting, and two informal intersessional meetings, between September 2019 and July 2020. Things were looking very good at the end of the second substantive session in February 2020. By that time, we had seen an exceptionally high level of participation from UN Member States and observers, as well as the buildup of a very positive dynamic among delegates. It had paid off to focus on issue presentations and discussions rather than on negotiations. When the OEWG began its work, the majority of delegations had never seriously engaged with cybersecurity in a UN context. It was important to give them the opportunity to familiarize themselves with the subject and its history in previous UN processes. I want to mention in particular, among the fresh voices that brought new energy to the deliberations on cybersecurity at the UN, the group of young female diplomats from various regions of the world, whose participation was encouraged and facilitated by the Women in International Security and Cyberspace Fellowship[5].

When the OEWG began its work, the majority of delegations had never seriously engaged with cybersecurity in a UN context.

Only a few days after the second substantive session, the disruptive force of the COVID-19 pandemic became all too obvious. Over the following months, we had to adapt the OEWG work plan several times. From traditional physical meetings we switched first to consultations by correspondence and then to a virtual format. Instead of July 2020, the third and final substantive session was held in March 2021 in a peculiar virtual/hybrid format. Fortunately, the mutual trust and overall positive momentum we were able to build prior to the pandemic did not dissipate during the period of virtual meetings, but carried us all to a successful conclusion of our mandate.

Aside from the impact of COVID-19, there were additional factors that complicated the process. The fact that the resolution establishing the OEWG was controversial and had to be voted on was obviously less than ideal. It was also a reflection of the current geopolitical environment, which is not exactly conducive to consensus on a global level. Furthermore, the new open-ended format, while offering the promise of new ideas and dynamics, required special efforts to create a reasonably level playing field for delegations.

There were also many elements that contributed positively to the process. The very high turnout was a strong indication of the rapidly growing awareness of cybersecurity threats, which has been exacerbated by the rapidly increasing number of cyberattacks on healthcare and scientific institutions since the COVID-19 pandemic outbreak. This certainly reinforced the general sense among delegations that progress needs to be made. More specifically, several delegations and individual delegates went above and beyond to contribute to the Group's success. The numerous proposals on the Group's website[6] are testament to this. Finally, the positive outcome would have been impossible without the technical expertise, institutional memory, and high availability of the UN support team (UNODA, UNIDIR, UNDGACM) under the leadership of the UN High Representative for Disarmament Affairs, Under-Secretary-General Izumi Nakamitsu.

The concurrent activities of the first OEWG and the sixth GGE did *not* prove to be a complicating factor, as some delegations had feared at the outset. The very different composition of the groups made for equally different approaches and working methods. In addition, the excellent relationship between the chair of the GGE, Ambassador Guilherme Patriota of Brazil, and myself was very help-

ful in avoiding any competition or contradictions between the two bodies. It is also noteworthy that the delegations who had voted against one resolution or the other in establishing the two groups nevertheless fully engaged once the work started. Ultimately, the processes and outcomes of the two groups were nothing but complementary and mutually reinforcing.

The OEWG concluded its work with a two-part report. The Final Substantive Report[7] contains those elements on which the delegations achieved consensus. Most importantly, it reestablished consensus on the 2015 acquis and it did so in a particularly meaningful way. In the past, the GGE reports had been agreed upon among the members of the Group and subsequently adopted by the General Assembly of the United Nations as a simple formality. In reality, beyond the members of the GGE, only a few delegations showed serious interest in the GGE's work or their reports. Meanwhile, with the OEWG, every Member State was offered the opportunity to contribute throughout the process and none would be able to pretend ignorance of its outcome. In this way, the OEWG has reaffirmed and significantly strengthened the existing normative framework. Beyond that, the Final Substantive Report contains various new elements that update and expand the acquis, of which I want to mention just a few examples.

The report provides a step forward in the Member States' assessment of the cyber threat landscape, as it mentions attacks on medical facilities and the need for their protection, also under the existing agreed-upon norms, as well as the impact of cyberattacks on healthcare infrastructure in the context of the COVID-19 pandemic. It recognizes the devastating humanitarian consequences of cyberattacks, and mentions practical measures as first steps toward building confidence, such as the designation of a national Point of Contact. Furthermore, the report recognizes the need for the protection of critical information infrastructures, including the need to ensure the general availability and integrity of the internet, often referred to as the public core of the internet. The strongest section of the report deals with capacity-building, in which it underscores the need for building cybersecurity capacity, pointing out that cybersecurity capacity-building is a two-way street, and offering a list of principles as guidance for capacity-building. The report also underscores the importance of narrowing the "digital divide," including the "gender digital divide," and pays tribute to the role of (non-governmental) stakeholders. In its last chapter, it recognizes the need for a regular, institutionalized forum for dialogue among States on the use of ICTs in the context of international security.

With the OEWG, every Member State was offered the opportunity to contribute throughout the process and none would be able to pretend ignorance of its outcome.

The Chair's Summary[8] contains those elements on which the delegations did not (yet) achieve consensus. It offers several orientations as well as a vast compendium of ideas and proposals that will encourage and enrich future discussions of cybersecurity. To name only a few, the collection of proposals for new norms, as well as the proposed guidance on the implementation of existing norms, will hopefully inspire future discussions. Readers may want to take a closer look at the actual document on the Group's website.

In addition to its actual outcome, the OEWG succeeded through its negotiation process in attracting attention and providing important impetus for accelerated engagement with the issue of cybersecurity by governmental and nongovernmental actors at the international, regional, and national levels.

Also, the above-mentioned inclusiveness of the OEWG went beyond the Member States and observers of the United Nations and opened a new chapter of stakeholder participation in an in

tergovernmental process on cybersecurity. While there is still room for improvement, non-state stakeholders played a much bigger role than in the past. Their presence and contribution were particularly strong during the Informal intersessional consultative meeting with Industry Partners and NGOs, which was held from 2 to 4 December 2019 in New York. Upon my request, the meeting was chaired by David Koh, Chief Executive of the Cyber Security Agency of Singapore, who submitted a separate Chair's Summary[9] that is annexed to the two-part OEWG report. Furthermore, the many written contributions by representatives of academia, non-governmental organizations, and the private sector from across the globe can be found on the Group's website. These contributions, as well as the numerous formal and informal formats of exchange with Member States, enriched the discussions of the OEWG and allowed for a more inclusive result, which is reflected among other elements in the references to a human-centric approach in cybersecurity and the importance of narrowing the gender digital divide.

OEWG went beyond the Member States and observers of the United Nations and opened a new chapter of stakeholder participation in an intergovernmental process on cybersecurity.

The successful conclusion of the OEWG came as a surprise to many and was generally welcomed with great relief and considerable satisfaction. However, as is usual in this type of exercise, hardly any delegation would declare—or openly admit—that they are completely satisfied with the result. Indeed, nobody got all their wishes. As Chair, I would have liked to have seen language in the report that was less prone to "UN speak" and better suited for public consumption. As Switzerland, we would have preferred an even stronger reference to the applicability of International Humanitarian Law. Pick any delegation and they will identify one or several shortcomings of the two-part report. In the end, none of the shortcomings seemed important enough to derail the process.

Herein lies one of the lessons we learned from the OEWG process: Multilateralism works! The delegations recognized the importance and urgency of addressing the issues relating to cybersecurity at a global level. After months of emphatic arguments and tough negotiations, they settled for compromise, because they knew that consensus was not a zero-sum game.

Meanwhile, the limits of that upon which Member States are currently willing to agree also became clear. Many fundamental differences persist, not all of which are exclusive to cybersecurity. One important difference pertains to the role of the international normative framework. Is the current framework sufficient for ICTs or does it require modifications or amendments? Should new norms be aspirational or immediately binding? In case of the latter, should their implementation be monitored by an international body, and should violations be sanctioned?

The OEWG process also offered a few early lessons in virtual diplomacy. As described above, the Group had a steep learning curve in the use of virtual conferencing platforms. In spite of several obstacles well known by anybody who may have recently been involved in international video-conferencing, the Group quickly adapted to the new tools, and the high participation and positive dynamic prevailed to the end. However, it is difficult to imagine this outcome if we had not had sufficient time before the outbreak of the pandemic to establish the necessary personal relationships and trust between delegates and between delegates and the Chair.

The discussion around cybersecurity has, fortunately, not stopped with the conclusion of the OEWG. Only a few weeks later, the GGE successfully finished its work, adding additional elements that will strengthen the normative framework for cybersecurity. In December 2020, the General

Assembly had already decided to establish a second OEWG, with a very similar mandate and a timeframe from 2021 to 2025. On 1 June 2021, the new OEWG held its organizational session and elected my former colleague, Ambassador Burhan Gafoor, the Permanent Representative of Singapore to the United Nations, as its Chair. In discussions during the first OEWG, many delegations expressed their hope that we would return to a single multilateral process on cybersecurity at the UN level. The new OEWG is likely to be able to play this role, as long as it is able to accommodate new ideas and proposals, such as the "Programme of Action," originally suggested by Egypt and France and now supported by many States from around the world. Also, the new OEWG needs to avoid being perceived as merely a "talk shop," but must deliver results well before its five-year mandate expires.

In addition to the work at the UN level, discussions and efforts to contain cybersecurity threats on regional and national levels are to be welcomed and supported. Such initiatives may deliver progress more quickly, and they are likely to offer valuable lessons for other regions or on a global scale. In this context, it was interesting to see that cybersecurity was one of the priority items on the agenda of the recent summit meeting between presidents Joe Biden of the United States and Vladimir Putin of Russia, which took place in Geneva, Switzerland. There is little doubt that any progress in their bilateral discussions on this topic would create a positive impetus to negotiations at the United Nations.

In any intergovernmental discussions on cybersecurity, be they on the international or regional level, States would have much to gain from better inclusion of stakeholders, such as the private sector, academia, and civil society. The area of international security and peace is particularly sensitive and remains by and large a core responsibility of states. Meanwhile, there is no denying that non-state actors play an important role, especially when it comes to cybersecurity, and that stakeholders have much to offer in terms of expertise and possible solutions. The above-mentioned Informal intersessional consultative meeting with Industry Partners and NGOs is an excellent example and proved to be a very fruitful encounter between (non-governmental) stakeholders and Member States. Much of its success is due to the excellent preparation of the event by the United Nations Office for Disarmament Affairs.

As much as the recent successes of the OEWG and the GGE are to be welcomed, the reality as reported in the media on an almost daily basis offers a bleaker picture. While diplomats succeeded in strengthening the international normative framework to promote responsible state behavior in cyberspace, the number and severity of violations of said framework by states and others seem to go up rather than down. The threat of escalation from "cyber incident" to open cyber conflict and beyond is rapidly increasing. Sooner rather than later, states will have to address issues such as attribution, accountability, and sanctions. Failure to do so may end up weakening the normative framework, as norms that are repeatedly violated with impunity carry little respect. In the meantime, efforts to strengthen confidence-building measures and capacity-building are more likely to succeed in the short term. Investments in the latter are urgently needed and likely to make a significant contribution to better prevention against malicious use of ICTs. All in all, the agenda of the OEWG seems just as relevant for future deliberations on developments in the field of information and telecommunications in the context of international security. The work never stops.

In any intergovernmental discussions on cybersecurity, be they on the international or regional level, States would have much to gain from better inclusion of stakeholders, such as the private sector, academia, and civil society.

Endnotes

1 United Nations General Assembly (75th session: 2020-2021). "Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security established pursuant to General Assembly resolution 73/27 of 5 December 2018". United Nations Digital Library, 2021. https://digitallibrary.un.org/record/3924426?ln=en.

2 United Nations General Assembly (73rd session). "Developments in the field of information and telecommunications in the context of international security". United Nations, December 5, 2018. https://undocs.org/en/A/RES/73/27.

3 The Resolution was eventually adopted in the UN General Assembly by 119 against 46 votes and 14 abstentions (among them Switzerland).

4 United Nations General Assembly (73rd session). "Advancing responsible State behaviour in cyberspace in the context of international security". United Nations, December 22, 2018. https://undocs.org/en/A/RES/73/266.

5 Please see: https://cybilportal.org/projects/women-and-international-security-in-cyberspace-fellowship/.

6 United Nations Office for Disarmament Affairs. "Open-ended Working Group". United Nations. https://www.un.org/disarmament/open-ended-working-group/.

7 United Nations General Assembly. "Open-ended working group on developments in the field of information telecommunications in the context of international security. Final Substantive Report". United Nations, March 10, 2021. https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

8 United Nations General Assembly. "Open-ended working group on Developments in the Field of Information and Telecommunications in the Context of International Security. Chair's Summary". United Nations, March 10, 2021. https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf.

9 Let's Talk Cyber. "Informal Multi-Stakeholder Cyber Dialogue. Summary Report". United Nations, December 04-10, 2020. https://front.un-arm.org/wp-content/uploads/2020/12/informal-ms-dialogue-series-summary-report-final.pdf.

About the Authors

Ambassador Jürg Lauber currently serves as the Permanent Representative of Switzerland to the United Nations Office and the other international organizations in Geneva. From 2015 to 2020, he served as Permanent Representative of Switzerland to the United Nations in New York. In parallel, he served as the Chair of the first UN Open-ended Working Group on developments in the field of information and telecommunications in the context of international security from 2019 until 2021. As a diplomat, he was previously posted in Bangkok, Bern, Beijing, Geneva, and New York. Between 2007 and 2009 he served as chef de cabinet to the President of the International Criminal Court. Before joining the Swiss Federal Department of Foreign Affairs in 1993, he worked in peacekeeping missions in Namibia (UNTAG) and Korea (Panmunjom).

Lukas Eberli served as the Adviser to Ambassador Jürg Lauber's Chairmanship of the UN OEWG from 2019 to 2021. He is currently holding the position as Second Secretary for Cybersecurity at the Permanent Mission of Switzerland to the United Nations and the other international organisations in Geneva. From 2019 until 2020 he was working at the Permanent Representation of Switzerland to the United Nations in New York, first covering Security Council issues and later Cybersecurity and Digital Cooperation. Lukas Eberli joined the Swiss Federal Department for Foreign Affairs in 2018, working at the Embassy of Switzerland in Jakarta, Indonesia. Before joining the Department, he worked as a political consultant for Members of the Swiss Federal Parliament.

Cyberstability Paper Series

New Conditions and Constellations in Cyber

Cybersecurity, Internet Governance, and the Multistakeholder Approach

The Role of Non-State Actors in Internet Policy Making

Wolfgang Kleinwächter
Professor Emeritus, University of Aarhus; Commissioner, Global Commission on Stability in Cyberspace (GCSC)

Cybersecurity, Internet Governance, and the Multistakeholder Approach: the Role of Non-State Actors in Internet Policy Making

Wolfgang Kleinwächter | Professor Emeritus, University of Aarhus; Commissioner, Global Commission on Stability in Cyberspace (GCSC)

In May 2021, Estonia chaired the UN Security Council (UNSC). It used its chairmanship to put the issue of cybersecurity under the so-called Aria-Format on the agenda. The discussion made clear: Cybersecurity is an issue of utmost importance for the world.[1]

Estonia, perhaps more than any other country, understands very well what cybersecurity means. It is one of the most developed digitalized countries, nicknamed e-stonia. It was the victim of a cyber-attack in 2007. It hosts the Tallin Manual, one of the most recognized guidelines for international cyberlaw. And it is the headquarters of the NATO Cooperative Cyber Defence Centre of Excellence.

When Estonian president Kersti Kaljulaid addressed the 76th UN-General Assembly (UNGA) on September 25, 2021, she said: "As an elected member of the Security Council, we were pleased to host the very first official discussion on cybersecurity in the Council, which allowed us to raise awareness on threats to international peace and security stemming from the malicious use of cyberspace and create momentum for the implementation of our existing framework. Discussions on cybersecurity and cybercrime must ensure that we make a concentrated effort to implement the rules of the road we already have." And she added: "We cannot go down this road without bringing companies and civil society along."[2]

This is a remarkable statement. It reflects the reality that, in our interconnected world, Internet-related national or international security issues are too big and too complex to leave them in the

Wolfgang Kleinwächter is a Professor Emeritus from the University of Aarhus, Commissioner in the Global Commission on Stability in Cyberspace (GCSC) and former ICANN Board member.

hands of governments alone. The Internet is developed by thousands of engineers, managed by tens of thousands of private entities, and used by more than four billion people around the world, regardless of frontiers. If governments want to find sustainable solutions for Internet-related issues, they will fail if they do not involve the developers, providers, and users of digital services in an appropriate way. When it comes to the governance of the Internet, there is no alternative to a multi-stakeholder approach.

The UN is an intergovernmental organization, and problems related to peace and international security are first of all a governmental affair. However, with global digitalization, the role of non-state actors in keeping cyberspace stable and safe is growing. With the extension of the mandate of the Open-Ended Working Group (OEWG) until 2025 (UN-Resolution 75/240), the United Nations has now started a process which will lead to something like a permanent forum in which to consider international cyber peace matters. One of the challenges for the new OEWG is how to ensure the regular and meaningful participation of non-governmental stakeholders and how to integrate them better into UN cyber dialogues.

Cybersecurity has been on the UN agenda since 1998. It was discussed in the process of the UN World Summit on the Information Society (WSIS). The "WSIS Tunis Agenda" (2005) reaffirmed "the necessity to further promote, develop and implement in cooperation with all stakeholders a global culture of cybersecurity."[3] However, within the 1st UNGA Committee, which deals with disarmament and threats to peace, the discussion of cybersecurity was seen as a privilege of governments. The six so-called "Groups of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security" (GGE) did not include non-state actors.[4] Nevertheless, the 2015 GGE report included a paragraph that stated: "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."[5]

This vague call to "identify mechanisms... as appropriate" was taken one step further in 2018 when the 73rd UNGA established an "Open-Ended Working Group" (OEWG). UN-Resolution 73/27 included in Paragraph 1.13 an obligation that "States should encourage the private sector and civil society to play an appropriate role to improve security of and in the use of ICTs, including supply chain security for ICT products and services." The resolution added, "States should cooperate with the private sector and the organizations of civil society in the sphere of implementation of rules of responsible behaviour in information space with regard to their potential role."[6]

When the OEWG started its work in September of 2019, many representatives from NGOs, civil society, the private sector, and the technical community were in the room. They did not have speaking rights, but before the official start of the sessions non-state actors did have fifteen minutes to raise issues, and they were allowed to distribute printed material to the governmental delegates.

The first formal OEWG meeting was followed by "informal consultations" in December of 2019. Non-state actors discussed on equal footing with governmental representatives. It was the first ever UN multi-stakeholder meeting on addressing cyberthreats in the context of international security. In his letter to the second formal OEWG meeting (March 2020), the Chair of the "informal consultation," Ambassador David Koh from Singapore, wrote: "The different perspectives provided by States, industry, civil society and academia were enriching and the concrete ideas put forward were constructive and innovative."[7]

While the Covid-19 pandemic changed the OEWG workplan and no further "informal consultations" took place, virtual meetings became the norm and opened new avenues for informal multistakeholder consultations.[8] In the Final Substantive OEWG Report, it says that "the OEWG has benefited from the expertise, knowledge and experience shared by representatives from inter-governmental organizations, regional organizations, civil society, the private sector, academia and the technical community."[9]

A resolution for a second OEWG with a mandate until 2025 was adopted, which "may decide to interact, as appropriate, with other interested parties, including businesses, non-governmental organizations and academia."[10]

It seems that there is now a general agreement that security in cyberspace can be achieved only if all stakeholders contribute in their respective roles. However, agreement on how and to what extent exactly they ought to be involved remains unclear. There are different ideas as to what is "appropriate" and how to organize the "interaction." The how is about access and speaking rights for business, civil society and the technical community. It is about the possibility of non-state actors to table their own proposals or to comment officially on governmental drafts. It is about the duty of governments to rationalize their decisions in public. Some governments want to keep the non-state actors at arm's length, others have no problems with including them in formal discussions. These are procedural issues. But the way in which non-state actors will be included in the forthcoming OEWG negotiations will have a substantial effect on possible outcomes.

It seems that there is now a general agreement that security in cyberspace can be achieved only if all stakeholders contribute in their respective roles. However, agreement on how and to what extent exactly they ought to be involved remains unclear.

Examples of how state and non-state actors can work hand in hand in promoting stability and security in cyberspace have emerged recently. The new Ad Hoc Committee (AHC), which works on a UN convention against cybercrime, has invited non-state actors "with expertise in the field of cybercrime," regardless of their formal recognition under ECOSOC rules.[11] In the negotiations on "Lethal Autonomous Weapon Systems" (LAWS), non-state actors such as the Campaign Stop Killer Robots, the Alan Turing Institute, or Amnesty International, are participating in regular meetings with speaking rights.[12]

There are other examples outside the UN-system of how multistakeholder cooperation has contributed to enhancing security and stability in cyberspace. The "Paris Call on Trust and Security in Cyberspace," initiated by the French government, is supported by seventy-nine governments, thirty-five local state authorities, 391 civil society organizations, and 706 private sector corporations.[13] It is not a legally binding document, but the political commitment, which is based on the work of the GGE, is very strong. Other multistakeholder cybersecurity projects are the "Tech Accord"[14] (Microsoft 2018), the "Charter of Trust"[15] (Siemens 2018), and the "Joint Civil Society Statement on Cyberpeace and Human Security" (2021). The Civil Society Statement was supported by the business community and called for "regular and meaningful participation of non-governmental stakeholders in the second OEWG and in any future UN forums."[16]

The "Global Commission on Stability in Cyberspace" (GCSC) is another example of fruitful multistakeholder collaboration. The GCSC Final Report, "Advancing Cybestability," has taken the eleven GGE norms[17] as a starting point and continued where governments stopped in 2015. It specified the norm on the protection of critical infrastructure by calling for a special norm to protect the "pub-

lic core of the Internet," it introduced a new norm to promote "Cyberhygiene," and it proposed that norms on behavior in cyberspace should not be only for states but also for non-state actors.[18]

Insofar as the OEWG has enough reference material to enhance the cooperation among state and non-state actors and to innovate cybersecurity negotiations within the UN, three options could be further considered:

1. **Informal consultations:** Between the formal OEWG meetings, informal consultations with non-state actors, regardless of ECOSOC-Status, would discuss related issues. A report of the informal consultations would be presented to the formal OEWG meetings. This would be the model for the first OEWG.
2. **Speaking rights:** Instead of separated informal consultation, non-state actors would get speaking rights in formal OEWG meetings, but would be excluded from formal negotiations. This would enhance the engagement of business, civil society, and the technical community beyond the first OEWG.
3. **Advisory Committee:** Non-state actors could be organized in three sub-committees, for business, civil society, and the technical community. Each of the sub-groups would have a small steering committee. The three chairs of the steering committee would form a "Troika," which could give advice to the formal OEWG meetings. Such a model was used by the WSIS. The WSIS Intergovernmental Bureau had regular exchanges with the business bureau (coordinated by the International Chamber of Commerce/ICC) and the Civil Society Bureau (coordinated by the Confederation of Non-Governmental Organisations/CONGO). Non-state actors did have speaking rights in plenary sessions and could participate as "silent onlookers" in negotiation groups.[19] Organizations such as the OECD[20] or ICANN have had a positive experience with similar advisory committees.

The new chair of the 2nd OEWG, Ambassador Burhan Gafoor from Singapore, signaled at the eve of the first OEWG meeting, scheduled for December, 13 – 17, 2021, a "positive" willingness to be more engaged with non-state actors. In his program of work, he indicated that he "is committed to engaging with stakeholders in a systematic, sustained and substantive manner" to find out "how the OEWG can engage them meaningfully and substantively in order to support discussions by member States and deliver tangible results." Participation of NGOs will be on a "non-objection basis". Ambassador Gafoor sees the precedent of the first OEWG as a starting point and he encouraged stakeholders to move forward towards new forms of "intermingling"[21].

The way in which the intergovernmental OEWG will organize its interaction with non-governmental stakeholders on its road toward 2025 could have an impact on the broader development of global governance in the "age of cyberinterdependence." There is no need to re-invent the wheel. There are numerous "best practice" examples that demonstrate how enhanced interaction among various actors with different legal status can help to find solutions for complex issues. The multistakeholder approach, which got its global recognition by the UN World Summit on the Information Society in 2005, is now recognized as the overriding principle for managing Internet-related public policy issues. And cybersecurity is one of the central issues on the long list of problems in our digital world.

Therefore it makes sense to look back at how, in the past, the interaction among state and non-state actors has been discussed and practiced, how the intergovernmental system, which was established after WWII, has evolved in the context of technological innovations with political implications, and how the multistakeholder governance model has been invented and designed step by step.

The question of how to organize the relationship between states and non-state actors within the UN is not new. Non-state actors are not excluded from the UN. Article 71 of the UN Charter gives the Economic and Social Council (ECOSOC) the mandate to "make suitable arrangements for consultation with non-governmental organizations which are concerned with matters within its competence."[22] The ECOSOC has recognized more than 4000 NGOs. In 1996 it specified in Resolution 1996/31 the criteria under which NGOs are recognized and how they should cooperate with UN bodies. The resolution makes a clear distinction between "participation" for states and "consultation" for NGOs.[23]

From a theoretical and legal point of view, this distinction is reasonable. However, in the globalized and interconnected world of the 2020s, such a distinction needs to be expanded toward a new quality of interaction. The challenges that come with the new complexity of cyberspace go beyond the capacity of individual governments to find sustainable solutions for new emerging issues. This does not change the legal status of the various actors. Non-state actors have different rights and responsibilities, but if governments want to find sustainable solutions, they need the engagement of all involved and affected parties. There is a need for a "holistic approach," which must include also new and innovative procedures for the interaction among state and non-state actors.

Many UN organizations have created avenues for an enhanced participation of non-state actors. UNESCO works with thousands of NGOs. The International Labour Organisation (ILO) is based on a tri-partite mechanism (governments, business, and trade unions). The International Telecommunication Union (ITU) opened its doors to so-called "private sector members" in 1994. But there is a "red line" when it comes to the negotiation table. In the ITU, sector members have an equal voice in the so-called "Study Groups," but they do not have a vote in the ITU Council or the ITU Plenipotentiary. Such "red lines" exist also in other UN bodies, such as the first UNGA Committee.

The way in which state and non-state actors cooperate within and outside the UN has been a topic of theoretical as well as political discussion for decades. When, in the early 1970s, new technologies challenged the established world, it was the "Club of Rome," which forecast that non-state actors will play a greater role in future global policy making.[24] In 1987, the futurologist Daniel Bell recognized that "the nation state has become too small for the big problems of life and too big for the small problems." He concluded that neither more centralization nor more decentralization should be the answer, but a diffusion of governance activities in several directions at the same time. Some functions "may migrate to a supra-governmental or transnational level. Some may devolve to local units. Other aspects of governance may migrate to the private sector."[25]

In 1991, Alvin Toffler, another futurologist, went one step further in his book "Powershift": "We live at a moment when the entire structure of power that held the world together is now disintegrating... it does not merely transfer power, it transforms it."[26] Joseph Nye from Harvard's Kennedy School of Government later mapped this in a matrix that illustrated "the possible diffusion of activities away from central governments, vertically to other levels of government and horizontally to market and private non-market actors, the so-called third sector."[27]

In 1995 the "United Nations Commission on Global Governance" defined this new concept of "Governance" in its report "Our Global Neighbourhood" as follows: "Governance is the sum of the many ways individuals and institutions, public and private, manage their common affairs. It is the continuing process through which conflicting or diverse interests may be accommodated and cooperative action may be taken. It includes formal institutions and regimes empowered to enforce compliance, as well as informal arrangements that people and institutions either have agreed to or perceive to be their interest."[28]

This new concept of "governance" also included civil society. In June 2004 the UN published a report of a "Group of Eminent Persons." Its chair, the former Brazilian President, Fernando Henrique Cardoso, wrote in his letter to UN Secretary General Kofi Annan: "The rise of civil society is indeed one of the landmark events of our times. Global governance is no longer the sole domain of governments. The growing participation and influence of non-state actors is enhancing democracy and reshaping multilateralism. Civil society organizations are also the prime movers of some of the most innovative initiatives to deal with emerging global threats. Given this reality, the Panel believes that constructively engaging with civil society is a necessity for the UN, not an option." They added: We see this opening up of the UN to a plurality of constituencies and actors not as a threat to governments, but as a powerful way to reinvigorate the intergovernmental process itself."[29]

The growing participation and influence of non-state actors is enhancing democracy and reshaping multilateralism. Civil society organizations are also the prime movers of some of the most innovative initiatives to deal with emerging global threats.

The discussions around new ways of "global governance" were primarily driven by the development of the Internet. The Internet started in the 1960s as a research project, financed by governmental money. However, unlike other communication technologies (telecommunication or broadcasting), it did not lead to state-owned companies or governmental regulation.

The governance of the Internet was described by Internet pioneers, such as the authors of the "Cluetrain Manifesto,"[30] as something like "governing without governments." In the early 1990s Dave Clark formulated the "Leitmotiv" of the Internet Engineering Task Force (IETF), the body that develops Internet protocols: "We reject: kings, presidents, and voting. We believe in: rough consensus and running code."[31] And the rock singer John Perry Barlow wrote in his "Davos Declaration of Cyberindependence" (1996) : "Governments of the Industrial World, you weary giants of flesh and steel. I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather."[32]

The Internet was indeed a revolution that changed everything. It has been compared to the invention of the printing press 500 years ago, which paved the way for the "industrial revolution" in the 18th and 19th centuries. However, the Internet is not just a "new communication technology"; it created a new infrastructure for a new society, which was called by the United Nations "the information society."

Neither can the Internet be compared with telecommunications nor with broadcasting. Both are centralized media. The Internet is a decentralized infrastructure. Telecommunications and broadcasting started as state monopolies within national borders. The Internet enabled an endless number of individuals and private institutions to innovate without governmental permission and regardless of frontiers. Telecommunications and broadcasting were highly regulated by national telecommunications and broadcasting laws. The Internet emerged in the shadow of governmental regulation and international geopolitics. There were no intergovernmental codification conferences to draft the TCP/IP protocols, to develop the global domain name system (DNS), or to create the World Wide Web. Delegations to manage a country code top-level domain (ccTLDs) were done by a handshake between Jon Postel and a trusted manager.

Regardless of this "private sector leadership," part of the truth is also that the Internet never did escape from the existing framework of national and international legislation. What was illegal offline

became not legal online. But it is also true that the procedures for the regulation of the technical components of the Internet and the philosophy behind "code making" are rather different from traditional "law making." Internet standards, codes, and guidelines, as described in the "Requests for Comments" (RFCs), did not come "top down" by a "majority voting" of elected representatives, but were drafted "bottom up" by respected and competent key players of the global Internet community, the concerned and affected constituencies, mainly the technical developers. "Rough consensus " was declared by the chair if the "humming" in the room was loud enough. [33]

The making of the Internet Corporation for Assigned Names and Numbers (ICANN) in 1998 is a good example of this new approach. ICANN has a mandate to manage a global public good and to allocate public resources as domain names and IP addresses. Its structure and procedures—a decentralized but coordinated mechanism that interlinks a broad range of constituencies from the private sector, the technical community, and civil society, organized in Supporting Organisations and Advisory Committees (SOAC)—enables an open, bottom-up and inclusive policy development process (PDP) and has created accountability and transparency mechanisms as safeguards for the public interest. ICANN mirrors the decentralized architecture of the Internet. All stakeholders have their voice.

Multistakeholder collaboration within ICANN does not create conflict-free zones. It is natural that different stakeholders have different interests. But the established procedures to find consensus have created a stable system that has demonstrated its sustainability.

ICANN is an innovation in the system of international relations. ICANN did not substitute other existing institutions; it added something new. ICANN is not the "world government of the Internet." ICANN was certainly inspired by the discussions around "cyberdemocracy" in the 1990s. But ICANN was never "governance without governments"; it was "multistakeholder governance with governments." Article 4 of ICANN´s "Articles of Incorporation" (1998) states: "The Corporation shall operate for the benefit of the Internet community as a whole, carrying out its activities in conformity with relevant principles of international law and applicable international conventions and local law and, to the extent appropriate and consistent with these Articles and its Bylaws, through open and transparent processes that enable competition and open entry in Internet-related markets. To this effect, the Corporation shall cooperate as appropriate with relevant international organizations."[34]

Within ICANN, the "Governmental Advisory Committee" (GAC), with its 160 members, is a special body. Different from the UN, governments have no decision-making power. It is the ICANN Board, representing the non-state constituencies of the SOACs, which makes decisions. Governments give advice. The GAC chair is a non-voting member of the ICANN Board, but without veto power. GAC advice is not legally binding. If the board rejects GAC advice, there is a mechanisms in place for mediation to find balanced solutions in the interest of the global Internet community.

The concepts of the "United Nations" (UN) and "United Constituencies" (ICANN) are two different governance models with different types of actors. They represent two different forms of social organizations with different legal status. In the early days of the Internet, those two worlds were rather separated. Public policy legislation was made in real places. Technical standard codification and resource allocation were made in virtual spaces. The two worlds clashed when the Internet penetrated nearly all spheres of the political, economic, and public life.

Table 1: Comparison of Multilateral and Multistakeholder Policy processes

Issue	Multilateral	Multistakeholder
Actors	Governments	Private Industry/Civil Society/ Technical Community
Structure	Hierarchies	Networks
Codification	National Laws and Intergovernmental Treaties	Universal Codes and Protocols
Mission	Broader political issues	Narrow technical issues
Policy Development	Top Down	Bottom Up
Decision Making	Majority Voting/Full Consensus	Rough Consensus
Representation	General Elections by all	Delegation by competent constituencies /NomComs
Participation	Restricted to authorized representatives	Free access/broad participation
Negotiations	Behind closed doors	Open and transparent
Result	Stability and Predictability	Flexibility

This clash started with WSIS in 2002. In WSIS, Internet Governance became the most controversial topic. While everybody agreed that there is a need for something like a global regulatory framework for the Internet, there was a wide range of different ideas about which kind of regulation should be developed and applied. Concepts of private sector self-regulation stood versus governmental regulation with a broad variety of co-regulatory ideas in between. The US argued that the Internet is managed by the private sector and it works. If it isn´t broken, don´t fix it. China disagreed and was calling for an intergovernmental treaty.[35]

In 2003 the UN Secretary General Kofi Annan established a multistakeholder "Working Group on Internet Governance" (WGIG), asking for help to bridge the controversy. In a speech during the Global Governance Forum in New York in March of 2004 he said: "The issues are numerous and complex. Even the definition of what is meant by Internet governance is a subject of debate. But the world has a common interest in ensuring the security and the dependability of this new medium. Equally important, we need to develop inclusive and participatory models of governance. The medium must be made accessible and responsive to the needs of all the world's people. In managing, promoting and protecting (the Internet's) presence in our lives, we need to be no less creative than those who invented it. Clearly, there is a need for governance, but that does not necessarily mean that it has to be done in the traditional way, for something that is so very different."[36]

Kofi Annan was calling for "innovation in policy making." WGIG was listening. The policy innovation that WGIG proposed was the multistakeholder concept. WGIG argued that the Internet does not need "leadership," it needs a "grand collaboration" of all involved stakeholders in their respective roles. It argued that "sharing" of policy development and decision making for Internet-related technical and public policy issues is more important than "fighting for leadership." WGIG also made clear that there is no "one size fits all" solution. New emerging issues should not be put into a pre-determined regulatory box. The governance model should be built around the specific needs

of a concrete issue. Bridging the digital divide, promoting digital trade, supporting cybersecurity, or managing the allocation of IP addresses would need specifically tailored governance mechanisms, which could and should be different. But sustainable solutions will be found only if all stakeholders are involved.[37]

In a multistakeholder process, each stakeholder brings its special expertise to the negotiation table. All stakeholders respect each other and meet on "equal footing" in their "respective roles." No stakeholder can substitute another stakeholder. Governments have a different role than business; civil society is different from the technical community. It is the complementary expertise, engagement, and responsibilities that create the beauty of the multistakeholder approach. All stakeholders need each other in the management of the global Internet Governance Ecosystem, a "virtual environment" comparable with our "natural environment" and the "rainforest."

In the "real rainforest," an uncountable number of diverse plants and animals live together in a very complex system. In the "virtual rainforest," we also have an endless and growing diversity of networks, services, applications, regimes, and other properties that co-exist in a mutually interdependent mechanism of communication, coordination, and collaboration. It is difficult to govern or control the rainforest, but parts of it can be damaged and destroyed. In the Internet Governance Ecosystem, many players with different legal status operate on different layers—at local, national, regional and international levels—driven by technical innovation, user needs, market opportunities, and political interests. As a result, we see a very dynamic process where—from a political-legal perspective—a broad variety of different regulatory, co-regulatory, or self-regulatory regimes emerge, co-exist, and complement or conflict with each other. The system as a whole is decentralized, diversified, and has no central authority. However, within the various subsystems there is an incredible broad variety of different sub-mechanisms that range from hierarchical structures under single or inter-governmental control to non-hierarchical networks based on self-regulatory mechanisms by non-governmental groups with a wide range of co-regulatory arrangements in between where affected and concerned stakeholders from governments, the private sector, civil society, and the technical community are working hand in hand.

A one-stakeholder approach risks ignoring the fundamental interests of other stakeholders. Technical issues could be pulled into political conflicts. Public interests could be sidelined by ignorance, selfish priorities, or profit interests. Even a two-stakeholder approach is risky. If big government and big industry go together, the risk is high that civil society interests will be sandwiched. If governments would go together with civil society by excluding the private sector, business models could collapse with negative consequences for economic growth, sustainable development, and future jobs. If civil society and the private sector would go together, they would soon miss the stability of a regulatory system. And without the technical community, the whole system would cease to function. In other words, if it comes to Internet governance, multistakeholderism is not one option, it is the only option.

The multistakeholder approach is the "policy innovation" for which Kofi Annan called in 2004. But the concept is still vague and needs further specification. There is no official definition of "multistakeholderism." There is no one single multistakeholder model. And it is unclear how rights and responsibilities are distributed among the stakeholders in concrete arrangements. Solutions will differ from case to case. While governments bear a primary role in cybersecurity, it is the private sector that has a primary role in the DNS management. But non-state actors have something to say in the field of cybersecurity, and governmental advice for managing the DNS—such as the introduction of new generic Top Level Domains (gTLDs)—is welcome.

The "Global Multistakeholder Meeting on the Future of Internet Governance" (Sao Paulo, April 2014) made an important step forward in further conceptualizing the multistakeholder approach. The "NETmundial Multistakeholder Statement" defined criteria for "Multistakeholderism," which now allows a certain "measurement." Such criteria include meaningful and accountable participation of stakeholders, in particular from developing countries and underprivileged groups, as well as open, participative, consensus-driven governance, transparency, accountability, inclusiveness, equitability, human rights and capacity building. The Sao Paulo statement did also say that "the respective roles and responsibilities of stakeholders should be interpreted in a flexible manner with reference to the issue under discussion."[38]

Another good example of a successful multistakeholder process was the IANA transition in 2016. The handover of the stewardship role of the US government for the Internet Root Server System to the global community demonstrated that all stakeholders can work together to the benefit of the global Internet community. The role of the US government and its oversight role over ICANN was one of the main conflicts during WSIS and the controversial discussions within two "UNCSTD Working Groups on Enhanced Cooperation" in the 2010s. There were many voices who did not believe that such a transition would ever happen. But it did.

The IANA transition negotiation process was a very innovative case of a new multistakeholder cyberdiplomacy. It produced an accountability mechanism and established the so-called "empowered community," which now has the final oversight over the management of critical Internet resources. Five years after the IANA transition, there is no doubt that the new system works. So far, there was no need to activate the "empowered community."

The established mechanism demonstrated its robustness when it was stress-tested by Covid-19. The pandemic triggered an explosive growth of Internet traffic and an extended need for more resources for domain names and IP addresses with all the Zoom conferences, home offices, distance learning, online shopping etc. But the good news was that the existing system could provide what was needed. There was no shortage on domain names and IP addresses; the public core of the Internet remained stable and delivered. The technical Internet did function.

The problems came with the use, or more specifically with the "misuse" of the resources. Cybercrime tripled; fake news and hate speech polluted the cultural environment. There was a new wave of government-sponsored cyberattacks. But those threats and risks appeared on the application layer. The transport layer—the DNS with its root and name servers—managed by the multistakeholder community, remained stable.

The multistakeholder concept is still in its early years. It is a journey into a political "terra incognita." It is a "trial and error" journey. There are a lot of strengths and opportunities, such as inclusion, sustainability, and conflict reduction. There are also weaknesses and risks, such as accountability, legitimacy, implementation, and compliance. It is certainly true that multi-stakeholder processes are more complicated and last longer than one-stakeholder processes, but the big plus comes with a higher degree of sustainability and flexibility, which allow for stumbling forward and for keeping the network open to accommodate tomorrow´s problems.

No doubt there is a need for more creativity and innovation. Kofi Annan´s plea, that for Internet policy making "we need to be no less creative than those who invented (the Internet)" is a permanent call for thinking out of the box. This call was also shared recently by ITU Secretary General Houlin Zhao in his address to the G20 Think Tank Summit (T20) in October of 2021 in Milan. When he pre

sented ITU´s "4I-Strategy" (Infrastructure, Investment, Innovation, Inclusion), he underlined that the call for "innovation" includes innovation in policy making.[39]

Unfortunately, the years after WSIS were wasted with more ideologically motivated conflicts. Groups that favored governmental leadership were calling for more "Multilateralism." Groups that favored private sector leadership were calling for more "Multistakeholderism." This was a senseless battle between "Isms." There is no conflict. Multilateralism and multistakeholderism are two sides of one coin. The multilateral (intergovernmental) treaty system is an important stabilizing factor in international relations, but in today´s world it is embedded in a multistakeholder environment. And multistakeholder arrangements, which are very often voluntary commitments, will benefit if core elements are translated into "hard law," which can only be made by governments and parliaments.

Multilateralism and multistakeholderism are two sides of one coin. The multilateral (intergovernmental) treaty system is an important stabilizing factor in international relations, but in today´s world it is embedded in a multistakeholder environment.

In the growing geo-strategic battles in cyberspace, the risk is high that the multistakeholder approach will be squeezed between hard political interests. This would be a big mistake. If cyberpowers ignore the complexity of the Internet governance ecosystem, they will fail to reach sustainable results and provoke zero-sum games that do not know any winners. All stakeholders will lose.

In the Internet, everything is connected with everything. Decisions on cybersecurity have economic implications and consequences for human rights. Regulation on privacy or freedom of expression affect business models and create problems for law enforcement. In the Internet world, all stakeholders are sitting in the same boat. With the next generation of technologies—Artificial Intelligence (AI) and the Internet of Things (IOT)—new threats and risks will emerge. The whole of mankind is sitting together in a boat that is moving toward a big waterfall. It makes no sense to start a battle within the boat. And it makes no sense to fight the waterfall. The common challenge is to stabilize the boat and to avoid a digital disaster.

Looking Forward toward 2025

Lessons learned from the multistakeholder processes are very relevant for all Internet-related public policy-making processes. And they are very relevant for future discussions around cybersecurity.

When UN Secretary General Antonio Guterres addressed the 14th IGF in Berlin (2019), not only did he support the multistakeholder approach, he offered the UN as a platform for multistakeholder discussion: "There's an absence of technical expertise among policymakers even in the most developed countries, invention is outpacing policy setting, and measured difference in culture and mindset are creating further challenges. ... while industry has been forging ahead and at times breaking things, policymakers have been watching from the sidelines. ... Let us build this fora into a platform where Government representatives from all parts of the world along with companies, technical experts and Civil Society can come together to share policy expertise, debate emerging technology issues, agree on some basic common principles, and take these ideas back to appropriate norm-setting fora."[40]

In his "Roadmap on Digital Cooperation" (May 2020), he proposed to strengthen the IGF toward an IGF+ and to add a high-level governmental and a parliamentarian track. For cybersecurity he proposed "a broad and overarching statement, endorsed by all Member States, in which common elements of understanding on digital trust and security are outlined...Following adoption by Member States, the statement could also be open to endorsement by stakeholders, such as those in the private sector, including technology companies, and civil society."[41]

In today's world, international security means cybersecurity. If a cyberattack against a state is interpreted as a threat or use of force under article 2.4 of the UN-Charter, it could trigger a real war. US President Joe Biden argued in a speech in July 2021: «We've seen how cyber threats, including ransomware attacks, increasingly are able to cause damage and disruption to the real world. I can't guarantee this, but I think it's more likely we're going to end up—well, if we end up in a war, a real shooting war with a major power, it's going to be as a consequence of a cyber breach of great consequence."[42]

Cyberdiplomacy, aimed at strengthening peaceful cooperation among states, will be more important than ever. But cyberdiplomats alone will not settle the problems. There is a need for enhanced cooperation among governmental and non-governmental stakeholders, with the aim to keep the cyberspace open, free, and secure and to create a peaceful digital environment for business, education, health, entertainment, and individual communication.

In his "Common Agenda" (September 2021), UN Secretary General Antonio Guterres has proposed a new "Global Digital Compact" among governments, the private sector, and civil society, which could be adopted at the "UN World Summit of the Future" in 2023.[43] Such a new compact would pave the way for the next big stop of the multistakeholder Internet governance and cybersecurity journey. In 2025 the UN has to review the Tunis Agenda and to decide upon the renewal of the IGF. And, by coincidence, in 2025 the mandate of the OEWG expires. 2025 will also mark the beginning of the last phase for the implementation of the UN Sustainable Development Goals (SDGs). The hope is that those decisions will pave the way into a future with cyberpeace and digital prosperity for everybody. There is no time to waste.

Endnotes

1 UN Security Council Arria-Formula Meeting, "The Impact of Emerging Technologies on International Peace and Security", United Nations, May 17, 2021, http://webtv.un.org/watch/un-security-council-arria-formula-meeting-on-%E2%80%9Cthe-impact-of-emerging-technologies-on-international-peace-and-security%E2%80%9D/6254689850001; See also, Megan Roberts, "The UN Security Council Tackles Emerging Technologies," Council on Foreign Relations, May 28, 2021. https://www.cfr.org/blog/net-politics

2 Kersti Kaljulaid, "Address by the President of the Republic of Estonia Kersti Kaljulaid at the 76th United Nations General Assembly," Permanent Mission of Estonia to the UN, September 22, 2021. https://estatements.unmeetings.org/estatements/10.0010/20210922/QsJ9c7IoOI5b/0MIpapckJNR0_en.pdf

3 "Tunis Agenda for the Information Society," ITU, November 18, 2005. https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html

4 See "Group of Governmental Experts," United Nations, https://www.un.org/disarmament/group-of-governmental-experts/. CT security awareness programmes designed to educate and inform institutions and individual citizens. Such programmes could be carried out in conjunction with efforts by international organizations, including the United Nations and its agencies, the private sector, academia and civil society organizations;

5 Group of Governmental Experts, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," A/70/174, United Nations, July 22, 2015. https://undocs.org/A/70/174

6 United Nations General Assembly, "Resolution adopted by the General Assembly on 5 December 2018 on Developments in the field of information and telecommunications in the context of international security", A/RES/73/27, United Nations, December, 5, 2018. https://undocs.org/A/RES/73/27

7 "Informal intersessional consultative meeting of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security, New York, 2-4 December 2019 (CR1), Chair's Summary," Reaching Critical Will, January 28, 2020, https://reachingcriticalwill.org/disarmament-fora/ict/oewg/documents

8 See for example the Let's Talk Cyber Discussions. The objective of the Informal Multi-stakeholder Virtual Dialogue Series is to support the ongoing discussions at the OEWG on developments in the field of information and communication technology (ICT) in the context of international security. Taking place in a new virtual format, it is an informal event at the initiative of the multi-stakeholder community and a number of UN member states. The dialogue series is intended to complement the OEWG, but it is not a formal part of the OEWG process. As a platform for dialogue between non-government organizations (NGOs), technical experts, civil society, the private sector and states, this series of thematic sessions aims to: Collect non-governmental stakeholder perspectives on the OEWG pre-draft, and create opportunities for in-depth dialogue between State and NGO communities on the themes of the OEWG. See also the two reports. "Let's Talk Cyber," https://letstalkcyber.org/

9 Open-ended working group on developments in the field of information and telecommunications in the context of international security, "Final Substantive Report," A/AC.290/2021/CRP.2, United Nations, March 10, 2021, https://www.un.org/disarmament/open-ended-working-group/

10 United Nations General Assembly, "Resolution adopted by the General Assembly on 31 December 2020 on Developments in the field of information and telecommunications in the context of international security," A/RES/75/240, United Nations, January 4, 2021 https://undocs.org/en/A/RES/75/240

11 Resolution 75/282 on Countering the use of information and communications technologies for criminal purposes: "8. Reaffirms that representatives of non-governmental organizations that are in consultative status with the Economic and Social Council, in accordance with Council resolution 1996/31 of 25 July 1996, may register with the secretariat in order to participate in the sessions of the Ad Hoc Committee; 9. Requests the Chair of the Ad Hoc Committee, in consultation with the United Nations Office on Drugs and Crime, to draw up a list of representatives of other relevant non governmental organizations, civil society organizations, academic institutions and the private sector, including those with expertise in the field of cybercrime, who may participate in the Ad Hoc Committee, taking into account the principles of transparency and equitable geographical representation, with due regard for gender parity, to submit the proposed list to Member States for their consideration on a non-objection basis and to bring the list to the attention of the Ad Hoc Committee for a final decision by the Ad Hoc Committee on participation; 10. Encourages the Chair of the Ad Hoc Committee to host intersessional consultations to solicit inputs from a diverse range of stakeholders on the elaboration of the draft convention; See: United Nations General Assembly "Resolution adopted by the General Assembly on 26 May 2021 on Countering the use of information and communications technologies for criminal purposes," A/RES/75/282, United Nations, June 1, 2021, https://undocs.org/en/A/RES/75/282, Based on this a "Call for applications to participate in the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes" was published. The 1st AHC meeting is scheduled for January 2022, see: United Nations Office on Drugs and Crime, "Call for Applications to Participate in the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes," United Nations, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/call-for-applications.html

12 "Statements from the 2021 CCW Group of Governmental Experts on lethal autonomous weapon systems, second meeting," Reaching Critical Will, September 24, 2021, https://reachingcriticalwill.org/disarmament-fora/ccw/2021/laws/statements

13 "Paris Call on Trust and Security in Cyberspace," Paris Call, November 12, 2019, https://pariscall.international/en/

14 "Tech Accord," Cybersecurity Tech Accord, April 17, 2018, see: https://cybertechaccord.org/

15 "Charter of Trust," Charter of Trust, February 2018, see: https://www.charteroftrust.com/

16 Joint Civil Society Statement on Cyber Peace and Human Security: " Ensure the regular and meaningful participation of non-governmental stakeholders in the second OEWG and in any future UN forums. Diverse actors have an established role to play in operationalizing and promoting the cyber norms and relevant international law, building capacity and resilience, and in monitoring and responding to cyber incidents. This experience and expertise needs to be better integrated into UN cyber dialogues", see: "Joint Civil Society Statement on Cyber Peace and Human Security at the 2021 UN General Assembly First Committee on Disarmament and International Security," Tech Accord, October 8, 2021, https://cybertechaccord.org/joint-civil-society-statement-on-cyber-peace-and-human-security-at-the-2021-un-general-assembly-first-committee-on-disarmament-and-international-security/

17 Group of Governmental Experts, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," A/70/174, United Nations, July 22, 2015, https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

18 Advancing Cyberstability: Final Report of the Global Commission on Stability in Cyber

space "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—cyberattacks. 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." See: Global Commission on the Stability of Cyberspace, "Advancing Cyberstability," The GCSC, November 2019, https://cyberstability.org/report/

19 See Wolfgang Kleinwaechter, "Multistakeholderism, Civil Society and Global Diplomacy: The Case of the World Summit on the Information Society," in Governing Global Electronic Networks: International Perspectives on Policy and Power, ed William J. Drake and Ernest J. Wilson III (Chicago & London: MIT Presse, 2004): pp. 535–582

20 The OECD, an intergovernmental organization of thirty-eight member states, has produced numerous reports and studies on cybersecurity. At the OECD Ministerial Conference in Seoul (2008) next to the already existing advisory committees for business and trade union two new advisory committees for civil society and the technical community were established. The Civil Society Information Society Advisory Council (CSISAC) facilitates the exchange of information between civil society organizations and the OECD Committee on Digital Economy Policy (CDEP) with the aim to contribute pro-actively to better informed policy decisions on digital issues. CSISAC has more than 100 institutional members and over 300 individual members. It is led by a Steering Committee that nominates a liaison as a point of contact between civil society and the intergovernmental CDEP. The CSISAC liaison and CSISAC Steering Committee can participate in the meetings of the CDEP which leads to better-informed and more widely accepted digital policies.

21 Burhan Gafoor, "Chair's Letter," United Nations, November 15, 2021. https://documents.unoda.org/wp-content/uploads/2021/11/OEWG-2021-2025_Chairs-letter_final.pdf

22 United Nations, Charter of the United Nations, October 24, 1945, https://www.un.org/en/about-us/un-charter/chapter-10

23 ECOSOC Resolution 1996/31, "Consultative relationship between the United Nations and non-governmental organizations": "20. Decisions on arrangements for consultation should be guided by the principle that consultative arrangements are to be made, on the one hand, for the purpose of enabling the Council or one of its bodies to secure expert information or advice from organizations having special competence in the subjects for which consultative arrangements are made, and, on the other hand, to enable international, regional, subregional and national organizations that represent important elements of public opinion to express their views. Therefore, the arrangements for consultation made with each organization should relate to the subjects for which that organization has a special competence or in which it has a special interest." See United Nations Economic and Social Council, "Consultative relationship between the United Nations and non-governmental organizations," United Nations, RES 1996/31, July 25, 1996. https://www.unov.org/documents/NGO/NGO_Resolution_1996_31.pdf

24 Donella Meadows et al., The Limits to Growth. A Report for the Club of Rome's Project on the Predicament of Mankind (New York: Universe Books, 1972)

25 Daniel Bell, "The World and the United States in 2013," Daedalus 116, no.3 (1987): 1-31. https://www.jstor.org/stable/20025107

26 Alvin Toffler, Powershift: Knowledge, Wealth, and Power at the Edge of the 21st Century (New York: Bantam, 1990): 229–230.

27 Joseph S. Nye, Jr, "Information Technology and Democratic Government," in Democra-

cy.com? Governance in a Networked World, ed Elaine Ciulla Kamarck and Joseph S. Nye, Jr. (Merrimack, NH: Hollins Publishing, 1999): 64

28 Commission on Global Governance, Our Global Neighborhood, 1995. See Jessica Erin Unterhalter, "Commission on Global Governance," Britannica, https://www.britannica.com/topic/Commission-on-Global-Governance

29 United Nations General Assembly, "Transmittal letter dated 7 June 2004 from the Chair of the Panel of Eminent Persons on United Nations–Civil Society Relations addressed to the Secretary-General" and "We the peoples: civil society, the United Nations and global governance. Report of the Panel of Eminent Persons on United Nations–Civil Society Relations," A/58/817, United Nations, June 11, 2004, https://undocs.org/A/58/817

30 Rick Levine, et al., The Cluetrain Manifesto: The End of Business as Usual (San Francisco: Basic Books, 1999)

31 Niels ten Oever and Kathleen Moriarty, "The Tao of IETF," IETF, last modified November 8, 2018. https://www.ietf.org/about/participate/tao/

32 John Perry Barlow, "A Declaration of Cyberindependence," Electronic Frontier Foundation, February 8, 1996, https://www.eff.org/de/cyberspace-independence

33 P. Resnick, "On Consensus and Humming in the IETF," IETF, RFC 7282, June 2014, https://datatracker.ietf.org/doc/html/rfc7282

34 ICANN, Articles of Incorporation of Internet Corporation for Assigned Names and Numbers, November 21, 1998 https://www.icann.org/resources/pages/articles-2012-02-25-en

35 Wolfgang Kleinwaechter and Daniel Stauffacher, The World Summit on the Information Society: Moving from the Past into the Future, (New York: United Nations ICT Task Force, 2005): 350.

36 Kofi Annan, "Internet Governance Issues are Numerous and Complex, Secretary-General Says at Opening of Global Forum," United Nations, March 25, 2004. https://www.un.org/press/en/2004/sgsm9220.doc.htm

37 Working Group on Internet Governance, "Report of the Working Group on Internet Governance," U.S. Department of State Archive, June 2005, https://2001-2009.state.gov/e/eeb/rls/rpts/othr/49653.htm

38 NETmundial, "NETmundial Multistakeholder Statement," NETmundial, April 24, 2014, https://netmundial.br/netmundial-multistakeholder-statement/

39 Houlin Zhao, "Speech by ITU Secretary General Houlin Zhao at the T20 Summit," Youtube, October 7, 2021 https://www.youtube.com/watch?v=V0VuAKjTrS8&t=2008s

40 Antonio Guterres, "Opening Speech, UN Secretary General Antonio Guterres at the 14th IGF," IGF, November 24, 2019 https://www.intgovforum.org/multilingual/content/igf-2019-%E2%80%93-day-1-%E2%80%93-convention-hall-ii-%E2%80%93-opening-ceremony-raw

41 UN Secretary-General, "Report of the Secretary-General. Roadmap for Digital Cooperation," United Nations, June 2020, https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf

42 Joe Biden, "Remarks by President Biden at the Office of the Director of National Intelligence," White House, July, 27, 2021, https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/07/27/remarks-by-president-biden-at-the-office-of-the-director-of-national-intelligence/

43 Secretary-General, "OUR COMMON AGENDA, Report of the Secretary-General," United Nations, September 2021, https://www.un.org/en/content/common-agenda-report/assets/pdf/Common_Agenda_Report_English.pdf

About the Author

Wolfgang Kleinwächter is a Professor Emeritus from the University of Aarhus, Commissioner in the Global Commission on Stability in Cyberspace (GCSC) and former ICANN Board member. He is involved in Internet Governance issues since the early 1990s. He was appointed by UN Secretary General Kofi Annan as a member of the WSIS Working Group on Internet Governance (2003-2005), served as Adviser to the chair of the Internet Governance Forum (2005-2010), Nitin Desai, and as Special Ambassador of the Net Mundial Initiative (NMI). He is the founder of the Summer School on Internet Governance (SSIG) and the European Dialogue on Internet Governance (EURODIG). He published more than ten book as "Internet Fragmentation: An Overview" (World Economic Forum Davos, 2017 with Vint Cerf and William Drake) and "Towards a Global Framework for Cyberpeace and Digital Cooperation: An Agenda for the 2020" with a preface from UN Secretary General Antonio Guterres (Berlin 2019). His blog is under Circle ID (http://www.circleid.com/members/5851/). In 2012, he got the "Internet Award" from the German Internet Economy Association (eco).

Cyberstability Paper Series
New Conditions and Constellations in Cyber

When Internet Governance Meets Digital Cooperation

Navigating IGF Growth and Development in the Context of an Evolving Internet Governance Ecosystem

Anriette Esterhuysen
Chair of the Multistakeholder Advisory Group of the United Nations Internet Governance Forum

Wim Degezelle
Internet Policy Analyst and Consultant

When Internet Governance Meets Digital Cooperation: Navigating IGF Growth and Development in the Context of an Evolving Internet Governance Ecosystem

Anriette Esterhuysen | Chair of the Multistakeholder Advisory Group of the United Nations Internet Governance Forum

Wim Degezelle | Internet Policy Analyst and Consultant

The UN Secretary-General talks about a new "more inclusive multilateralism" in his report, entitled "Our Common Agenda."[1] This should not lead to a debate on multi-lateral versus multistakeholder approaches. "Multilateral" refers to a system with its own legitimacy and failings. "Multistakeholder" is an approach, not a substitute for accountable governance. It is a way of creating more learning and understanding through dialogue between different types of stakeholders with different perspectives and interests. Whether a global internet-related decision-making process is multistakeholder, or led by governments in a multilateral arena, the extent to which it is supported by open and inclusive debate will impact the effectiveness and sustainability of its outcomes. The Internet Governance Forum (IGF) has been and continues to be the most open, diverse, and inclusive space for multistakeholder dialogue on Internet-related policy, including in the context of broader digital cooperation. The IGF is currently in its 16th year, with renewal of its mandate[2] by the UN General Assembly scheduled for 2025. The Forum, on which Member states

Anriette Esterhuysen is currently the Chair of the Multistakeholder Advisory Group of the United Nations Internet Governance Forum. She is a Commissioner on the Global Commission on the Stability of Cyberspace and is the former executive director of the Association for Progressive Communications.

Wim Degezelle is an independent Internet Policy Analyst and Consultant with over 20 years' experience.

agreed at the conclusion of the World Summit on the Information Society (WSIS) in Tunis in 2005, has grown and evolved extensively since its first iteration in Athens in 2006—in scope, reach, format, and scale. So has the Internet. In 2005, the concept of the Internet as a network of networks was still abstract to many UN Member states. Nowadays, the Internet and related issues have priority on many policy agendas. Having grown from 1.1 billion users in 2005 to more than 4 billion users today,3 the Internet is at the center of a process of digitalization that is transforming the workplace, social and political processes, business, and trade, as well as people's personal lives. Many of the policy questions that were on the table in 2005 are still priorities today. Access to the Internet and information and communication technologies remains extremely unequal, between and within countries and regions. The availability and affordability of infrastructure, devices, content, language, and the human capacity needed to reap the benefits of using the Internet remain key Internet governance challenges.

At the other end of the spectrum, hyper-connectivity and the resulting dependence on Internet-based systems and services are presenting new challenges, threats, and risks. A stable and secure Internet is more important than ever before. Downtime or failure may have a real economic impact or even human cost. New developments and technological trends that use the Internet in combination with, for example, the Internet of Things, datafication, artificial intelligence, machine learning, and automated decision making, create a whole new range of policy challenges. The common denominator is that the range of Internet-related policy and regulation issues continues to expand, cross borders, and intersect with other spheres. Linked to this is a proliferation of venues that deal with Internet-related issues; some of these are new venues, but many are not, and pre-date the Internet, for example national legislatures, regulators, competition commissions, human rights institutions, and those dealing with peace and security. What is new is that they must give serious attention to Internet-related aspects of their areas of work.

Is the IGF still needed when Internet governance issue are being discussed everywhere? And how can the IGF evolve to remain relevant? The aim of this article is not to add yet another wish list to the existing body of ideas on strengthening the IGF; rather, it aims to point out where ideas can be consolidated, where strategic choices will have to be made between conflicting visions, and where attention needs to be given to the IGF's institutional configuration and capacity.

The IGF's broad mandate in the Tunis Agenda[4] and its unique identity as both part of the UN, but not bound by member-state driven processes in a narrow sense, allowed it to create a space where different stakeholder groups[5] can table and debate policy challenges in an atmosphere of open dialogue[6] without the pressure and limitations presented by having to negotiate agreed outcomes. There was no template for this kind of forum in the UN system and this encouraged innovation from the outset. The steady growth of the IGF demonstrates the need for a forum for open dialogue about Internet governance.[7] Its unique value stems from its ability to serve as a place where issues can emerge, be examined and debated from diverse perspectives, and thus be better understood before they move to spaces for more in-depth consideration and decision making. Bringing discussions to the IGF prevents issues from being discussed in parallel silos, without cross linkages and the exchange of ideas. Because it is inclusive and accessible, the IGF can avoid situations in which the views of those who do not have access to more specialized policy forums are ignored. "Community input" on the program content and organization of the annual meeting has grown into a central pillar of the IGF process. Early on the IGF introduced Open Consultations[8] and calls for input from participants and other interested stakeholders. It is

The steady growth of the IGF demonstrates the need for a forum for open dialogue about Internet governance.

complemented by a "stock-taking" session on the final day of the annual meeting where participants have access to an open microphone and can share what worked for them, and what they felt should change.[9] As a result, community input has also been the driver for the Multistakeholder Advisory Group (MAG)[10] and the IGF Secretariat[11] to introduce new elements into the IGF process.[12] Innovations such as regional, and later national IGFs, and Internet Governance Schools, emerged outside of the IGF itself, but soon formed strong links with the global process. The first Dynamic Coalitions—open, multistakeholder communities of practice dedicated to an Internet governance issue or set of issues—emerged at the first IGF meeting, held in Athens in 2006. Best Practice Forums (BPFs) were introduced to gather existing and emerging solutions to specific internet policy-related challenges. Through the organic growth of national and regional IGFs, the IGF process has found a way of responding to a challenge that applies to all global governance processes: effective linkages between national, regional, and international levels.

So, how can the IGF evolve to remain relevant? Innovating in response to received input is a key part of the answer, but it is not enough. The strength of relying on the "bottom up" approach to discuss IGF evolution is two-fold: it is responsive to expressed needs, and involves stakeholders dealing with policy as well as those participating in implementation. Its weakness lies in the fact that discussions do not easily lend themselves to introducing changes of a more strategic, or structural nature, such as, for example, how to effectively relate to other institutions, including governments, and multilateral processes. To remain relevant, the IGF needs the leadership and institutional capacity to represent the IGF, assess proposals for improvements strategically, implement them, and ensure that all the different elements of this growing IGF ecosystem work in a complementary manner toward achieving clearly articulated goals.

Discussions and ideas for improving the IGF are as old as the IGF. In what follows, the article highlights some of the most promising suggestions for improving the IGF from three sources: WSIS-processes (2012–2016), the IGF MAG Working Group on IGF Strategy and Strengthening (2020–21), and the UN Secretary-General's Roadmap for Digital Cooperation and Common Agenda (2020–2021). As mentioned before, responding effectively to these concrete calls for improvement requires identifying where ideas can be consolidated, where strategic choices have to be made, and where attention needs to be given to the IGF's institutional configuration and capacity.

The United Nations Conference on Trade and Development (UNCTAD) Commission on Science and Technology for Development (CSTD) reviews the implementation of and follow-up on WSIS outcomes, including the IGF, which has been the subject of intense debate. The CSTD became the arena in which UN member states supporting the multistakeholder approach argue with those in favor of more oversight by governments.[13] IGF supporters would point to its inclusiveness, the large number of participants, and the strong program content. IGF critics say that IGF was not a decision-making body, produced no clear outcomes, and that governments were not effectively represented. In July 2010 the CSTD established a multistakeholder Working Group on Improvements to the IGF to recommend improvements in line with the Tunis Agenda mandate, based on input from Member states and others.[14] In its report the Working Group homed in on broadening participation, producing more tangible outputs, strengthening links to other IG entities, and ensuring the IGF Secretariat has sufficient capacity.[15]

An "IGF retreat,"[16] convened by the UN DESA in July 2016, in the aftermath of the IGF's mandate renewal,[17] affirmed the CSTD Working Group's recommendations. The retreat's report added in more detail to the recommendations and is rich in suggestions, but unfortunately remains short on specifics of who should be taking things forward.

Perspectives on the extent to which the recommendations of the CSTD Working Group have been implemented vary.[18] It is worth noting that many of these recommendations resurfaced in the report of the Secretary-General's High-Level Panel on Digital Cooperation, and, to some extent, also in the Roadmap. Both documents are addressed below.

In 2020 the UN Secretary-General published the Roadmap for Digital Cooperation,[19] which includes a broad range of action areas, from trust and security to artificial intelligence and digital inclusion.[20] It recognizes the growing complexity and diffusion of the existing digital cooperation architecture, observing that "global discussions and processes are often not inclusive enough," nor, necessarily, effective, and that this "is exacerbated by the lack of a common entry point into the global digital architecture, which makes it especially hard for developing countries, small and medium-sized enterprises, marginalized groups, and other stakeholders with limited budgets and expertise to make their voices heard."[21]

Its holistic approach to digital cooperation makes the Roadmap a significant document. At the same time, it is striking that the IGF, a forum where Internet-related public policies are approached holistically and discussed openly, does not have a more prominent place in the Roadmap implementation. This is even more surprising considering that the source document for the Roadmap, the Report of the UN Secretary-General's High-Level Panel on Digital Cooperation (HLPDC), "The Age of Digital Interdependence,"[22] proposes an evolved IGF as one of the options for an over-arching mechanism for global digital cooperation.[23] The suggestions—outlined in paragraph 93 (a) of the Roadmap—include ideas that echo the CSTD WG's recommendations, but do not acknowledge that several were already being implemented by the IGF Secretariat and the MAG. In addition, the Roadmap introduced the idea, which provoked quite some controversy, of a new and empowered multistakeholder high-level body. Paragraph 93 (a):

> a) Creating a strategic and empowered multistakeholder high-level body, building on the experience of the existing multistakeholder advisory group, which would address urgent issues, coordinate follow-up action on Forum discussions and relay proposed policy approaches and recommendations from the Forum to the appropriate normative and decision-making forums; (b) Having a more focused agenda for the Forum based on a limited number of strategic policy issues; (c) Establishing a high-level segment and ministerial or parliamentarian tracks, ensuring more actionable outcomes; (d) Forging stronger links among the global Forum and its regional, national, subregional, and youth initiatives; (e) Better integrating programme and intersessional policy development work to support other priority areas outlined in the present report; (f) Addressing the long-term sustainability of the Forum and the resources necessary for increased participation, through an innovative and viable fundraising strategy, as promoted by the round table; (g) Enhancing the visibility of the Forum, including through a stronger corporate identity and improved reporting to other United Nations entities.

In a reaction to the Roadmap, the MAG Chair, in cooperation with the Government of Switzerland, organized a "Roadmap" session during the First Open Consultations on IGF 2020,[24,25] and the MAG established a working group on Strategy and Strengthening to act as a focal point for its participation in the Roadmap process. During 2020, the MAG Chair, in collaboration with the working group, convened a series of online discussions[26] on topics such as expanding participation in the IGF, making the IGF more multilingual, integrating more effectively with national and regional and youth IGFs, and learning lessons from several years of working with Best Practice Forums[27] and Dynamic Coalitions.[28] In September 2020, and based on extensive consultation with different

stakeholders, the Governments of Germany and the United Arab Emirates[29] submitted a paper called "Options for the Future of Digital Cooperation" to the UN Secretary-General,[30] which affirms the idea of the IGF being central in the architecture of digital cooperation. The way forward should rest on maintaining and upgrading the IGF's existing structures and making the organization more outcome-oriented. Their vision is for the IGF to be "a facilitator which connects existing discussions that are already taking place," and that the discussions at the IGF result "in action-oriented, but non-binding recommendations or reports" to ensure that they can find their way into policy-making processes.[31]

The UN Secretary-General's interest in the IGF, even if some proposals such as the multistakeholder high-level body raised questions, encouraged the supporters of the IGF and multistakeholder approach. This positive reaction was voiced, for example, in the IGF 2019 Main Session on Internet Governance and Digital Cooperation,[32] the January 2020 Open Consultation,[33] the IGF 2020 Main Session on the Roadmap for Digital Cooperation,[34] and the work of the MAG Working Group on IGF Strategy and Strengthening. It was evident that governments who supported the IGF were also deeply invested in the forum taking on and responding to the Roadmap, as illustrated through the Options Paper discussed below. The IGF MAG, through the MAG Working Group on IGF Strategy, formulated, apart from a comprehensive set of operational suggestions for IGF 2021, longer-term strategic measures by which to achieve a more strategic, inclusive, and impactful IGF. These include proposals to adopt a multi-year planning cycle[35] and a more consistent issue-driven approach to IGF program development; strengthen, develop, and integrate the IGF's intersessional activities (BPFs, DCs, NRIs, and now Policy Networks); consolidate integration of national legislators through an IGF Parliamentary Track; consolidate liaison with decision-making bodies; and strengthen communications strategies and mechanisms.[36]

The UN Secretary-General's interest in the IGF, even if some proposals such as the multistakeholder high-level body raised questions, encouraged the supporters of the IGF and multistakeholder approach.

They also responded with specific proposals on how to operationalize the proposed new multistakeholder high-level body which was discussed in detail in the Options Paper.[37] In 2021 the Secretariat introduced a new modality, policy networks, to the IGF ecosystem which can be said to respond to the "policy incubator" and "cooperation accelerator" ideas in the HLPDC's IGF plus model.[38] Two policy networks, one on the "environment" and one on "universal access and meaningful connectivity," were launched in the first half of 2021 with the intention of developing specific recommendations related to their focus areas. The Secretariat also embarked on a capacity-building program—an initiative they started long before the Roadmap was published, which included a report the Secretariat commissioned in 2019 on an IGF framework for capacity development. This responds to a recommendation originally made in the CSTD Working Group on Improvements to the IGF. Other components of the IGF that definitely respond to the Roadmap are the high-level leaders sessions, which have grown in scope since the first one in 2011, and the parliamentary track, which started in 2019. These add to the weight of the IGF and bring policy makers into the process, but they can also easily become isolated from the broader, more inclusive IGF process.

In November 2021, after doing its own round of further consultations on the proposed high-level body,[39] the IGF Secretariat published, at the request of the Executive Office of the United Nations Secretary-General, a public call for nominations for members and terms of reference for what has been named the "IGF Leadership panel."[40] It will consist of ten members to be appointed by the Secretary-General, drawing on a pool of candidates nominated by all IGF stakeholder groups.[41]

The Chair and Vice-Chair of the Group will rotate among members of the group, elected by members of the group. The role of the Leadership Panel will be to address strategic and urgent issues, highlighting Forum discussions and possible follow-up actions to promote greater impact and dissemination of IGF discussions. Its responsibilities are to provide strategic input and advice on the IGF; promote the IGF and its outputs; support both high-level and at-large stakeholder engagement in the IGF; and exchange IGF outputs with other stakeholders and relevant fora, also facilitating input of these decision-makers and fora into the IGF's agenda-setting process.[42] The terms of reference outline relations between the Panel and the MAG, saying that "the two bodies will function as distinct entities" to ensure there is no overlap between them, but that they should work "with close linkages and continuous efforts to promote collaboration and cooperation within the IGF."[43] The MAG will lead on the IGF annual work program and the global forum while the Panel will "contribute strategic inputs to the programme-setting and support the visibility of the IGF" and "provide high-level input and promote IGF outputs." The panel will be supported by the Secretariat. In several respects, the panel's terms of reference do respond to the proposals in the Options Paper. Relations with the MAG are less clear. What is most unclear is whether the Leadership Panel will have any authority in relation to the IGF Secretariat and to others inside the UN responsible for the IGF.

Put simply, the terms of reference for the Leadership Panel describe the main role of the IGF MAG as being to gather input from the community and plan the IGF's annual work program, while that of the Leadership Panel is to increase the IGF's visibility and promote its outputs to decision-makers.

As with earlier sets of recommendations, what remains unclear is where precisely oversight and institutional responsibility—and accountability—for following up on recommendations for IGF strengthening is located. The assumption is that it lies with the Department for Economic and Social Affairs of the United Nations (UN DESA), the UN department entrusted with supporting and overseeing the IGF, but how this oversight layer relates to the Leadership Panel is as unclear as has been the case with regard to the MAG.

In late 2020 the Office of the Secretary General's Envoy on Technology[44] was established[45] to lead implementation of the Roadmap, working closely with various United Nations entities and organizations from civil society, business, and the technical community. More recently, the Office has also been assigned with responsibility for parts of the Common Agenda (published in September 2021 and discussed below). According to its website, the Office of the Envoy is intended to serve "as an advocate and focal point for digital cooperation so that Member States, the private sector, civil society, academic and technical communities, and other stakeholders have a first port of call for the broader United Nations system,"[46] and is expected to work closely with the IGF community and with UN DESA to strengthen the IGF.[47] However, in spite of the active participation in IGF events by members of staff of the Office, and some presence of UN DESA and IGF staff in Roadmap processes, the implementation of the Roadmap process has largely bypassed the IGF. It has certainly not used the extended IGF ecosystem (National and Regional and Youth IGF Initiatives, BPFs, Policy Networks, and Dynamic Coalitions) in its roll-out process. This might change once the Leadership Panel starts its work, as the Envoy will be an ex-officio member.

In September 2021, on the occasion of its 75th anniversary, the UN Secretary-General presented his report—entitled "Our Common Agenda"—to the General Assembly.[48] This visionary and ambitious document "builds on and responds to the declaration on the commemoration of the seventy-fifth anniversary of the United Nations, in which Member States made 12 critical commitments: to leave no one behind; to protect our planet; to promote peace and prevent conflict; to abide by

international law and ensure justice; to place women and girls at the centre; to build trust; to improve digital cooperation; to upgrade the United Nations; to ensure sustainable financing; to boost partnerships; to listen to and work with youth; and to be prepared for future crises, including but not limited to public health crises."[49,50]

The IGF is presented with a challenge, but also with a massive opportunity. The challenge is clear in paragraph 93 of the Common Agenda : "It is time to protect the online space and strengthen its governance. I would urge the Internet Governance Forum to adapt, innovate and reform to support effective governance of the digital commons and keep pace with rapid, real-world developments."[51] The opportunity follows when the Secretary-General proposes that, building on the Roadmap, the United Nations, Governments, the private sector, and civil society come together "as a multistakeholder digital technology track in preparation for a Summit of the Future to agree on a Global Digital Compact." This Compact[52] "would outline shared principles for an open, free and secure digital future for all."[53] The issues the Secretary-General lists to be addressed by this Compact are all issues that have been, and continue to be, central to discussions at the IGF: "reaffirming the fundamental commitment to connecting the unconnected; avoiding fragmentation of the Internet; providing people with options as to how their data is used; application of human rights online; and promoting a trustworthy Internet by introducing accountability criteria for discrimination and misleading content" and "promoting regulation of artificial intelligence to ensure that this is aligned with shared global values."[54] It is striking, again, that the text of this document does not, in any way, gives recognition to the fact that the IGF has constantly adapted and innovated and that it has made a substantial contribution to the international community's understanding of challenges related to digitalization and cooperation in responding to such challenges.

In fact, measures and initiatives to strengthen the IGF that are taken by the Secretariat, MAG, and UN DESA seem to have remained largely unnoticed, even within the UN system. This raises questions as to whether these measures have been communicated effectively as serious responses to the calls for strengthening and improving the IGF, and as part of a longer-term strategic vision of an IGF for the future.

Nevertheless, exploring what the Secretary-General means by "adapt, innovate and reform" and "supporting effective governance of the digital commons" might mean that the IGF remains relevant, particularly considering the relatively open-ended nature of IGF evolution and improvement over the last decade.

The opportunity for the IGF to be the leading platform for engagement and consultation on the proposed Global Digital Compact is appealing. What is not clear, however, in the Common Agenda but also in other documents, including the terms of reference of the new Leadership Panel, is who is being addressed as the "IGF." Is it the MAG, the Secretariat and UN DESA, the components of the extended IGF ecosystem, or participants in the IGF process? The implication is that it is all of these, and therein lies the fault line: responsibility and accountability are not clearly allocated. As mentioned above, a core feature of the IGF is its bottom-up nature, which constantly leads to evolution and innovation in the margins. Although there certainly is an "IGF community," that community is particularly diverse, open, and is made up of voluntary contributions—both in the form of time and through financial support. The political, intellectual, and networking capital represented by this community is immense. What the IGF lacks is clear institutional identity, accountable leadership and management, and the human resources with which to facilitate linkages within this community and between the IGF and other components of the IGF ecosystem, including within the UN system. Neither the Leadership Panel nor the MAG have any kind of overarching role with regard to the IGF as an organization (or institution).

Some of the proposals in the Roadmap are covered by the terms of reference of the Leadership panel, such as increasing the visibility of the IGF and communicating IGF outputs. Some, such as "(b) Having a more focused agenda for the Forum based on a limited number of strategic policy issues," "(d) Forging stronger links among the global Forum and its regional, national, sub-regional and youth initiatives," and "(e) Better integrating programme and intersessional policy development work,"[55] are covered by the MAG's terms of reference. But ultimately both the Leadership Panel and MAG's roles are only advisory. Based on the published terms of reference, the Leadership Panel is not being charged with overseeing the Roadmap proposal to enhance the visibility of the Forum "through a stronger corporate identity and improved reporting to other United Nations entities."[56] If the organizational structure[57] of the IGF still included an Executive Coordinator[58] that led the Secretariat, as was the case up to 2010, and a Special Advisor chairing the MAG,[59] these advisory bodies would be able to interact with clearly accountable internal leadership and management.

What the IGF lacks is clear institutional identity, accountable leadership and management, and the human resources with which to facilitate linkages within this community and between the IGF and other components of the IGF ecosystem, including within the UN system.

Should the mandate of the IGF be reviewed? This question might come up in the course of negotiations on the renewal of the IGF's mandate in 2025. The answer has implications for the improvements to be logically pursued in the remainder of the current mandate. The IGF mandate outlined in the Tunis Agenda emphasizes an open and inclusive process, a "multistakeholder policy dialogue" on "issues related to key elements of Internet governance in order to foster the sustainability, robustness, security, stability, and development of the Internet" and "discourse between bodies dealing with different cross-cutting international public policies regarding the Internet."[60] The mandate also instructs the IGF to "discuss issues that do not fall within the scope of any existing body" and to interface with appropriate inter-governmental organizations and other institutions on matters under their purview."[61] The current mandate does not stand in the way of answering calls for strengthening the IGF in the Roadmap, or playing the role envisaged for it in the Common Agenda. The IGF mandate outlined in the Tunis Agenda remains fit for purpose and should be extended. It might be worth considering—in light of the broader scope of issues under discussion—changing the name of the IGF from "Internet Governance Forum" to "Digital Governance Forum."

Are current efforts to evolve the IGF going in the right direction? Or are they simply contributing to spreading the IGF Secretariat and MAG's resources even more thinly? Both assertions are true. Recommendations by the CSTD, efforts emanating from the Digital Cooperation process, and the Office of the UN Secretary General's Envoy on Technology have served to elevate the relevance of digital development and cooperation. The holistic approach of the Roadmap reflects the broad approach to Internet governance taken by the WSIS and in the program content of the IGF. In other respects, however, the Roadmap process does not seem to consider the IGF as an effective platform for facilitating cooperation and engagement of its own action plan. If the Leadership Panel can operate in a manner that complements the IGF MAG, and that can help fill the leadership gap in the IGF mentioned above, it could definitely contribute to a stronger IGF. If not, it could just spread the financial and institutional resources of the Secretariat even more thinly than is already the case. If its role is to promote particular policy approaches that emerge from IGF discussions, it is likely to reinvigorate previous critiques of the IGF and the demand for "enhanced cooperation" as a distinct process.[62]

Should the IGF continue to diversify or consolidate?
In the last decade, what is referred to as the "IGF ecosystem" has diversified, with around 140 national and regional IGFs, youth IGF initiatives, Best Practice Forums, Dynamic Coalitions, Policy Networks, and IGF capacity-building framework. Providing these activities with effective support, and ensuring that they all remain inclusive, interactive, and focused, is a massive challenge. The IGF either needs to consolidate the current diversification of intersessional activities but with a stronger capacity to "connect the dots" and do effective outreach and communications, or it might be better off by just being a very inclusive annual event with more focused content.

Regardless of the choice, the IGF should maintain its open, bottom-up character; cooperate and partner with other institutions; be more inclusive (and there are different angles to this, from language to region, to discipline, to Internet governance insiders and outsiders); focus the subject matter it discusses (which would also make it easier to establish continuity between annual meetings and avoid the annual events that are stand-alone events, silos on their own); be able to navigate multistakeholder and multilateral forums and, most importantly, acts as a place for them to connect with one another and facilitate other people's navigation across these spaces. The IGF is, and continues to be, the only existing, and in the authors' view, the only viable interdisciplinary, global, multistakeholder platform for open and inclusive engagement and public participation in Internet governance.

Filling in the leadership gap in the IGF. This can be done by filling in the role of IGF Executive Coordinator, by appointing a new person in this role, or by promoting the current head of the Secretariat to this position. This will provide clear and empowered executive leadership within the IGF's organizational layer, which can work with both the MAG and the Leadership Panel and assume accountability for operationalizing strategic advice received from these bodies and from the broader IGF community. The role of the Special Advisor is also important and it remains to be seen whether the Leadership Panel will be an effective substitute.

Focus on longer-term strategic planning, implementation, monitoring and evaluation of the IGF. The Secretariat is the center of the entire IGF ecosystem. As this ecosystem grows, and as the IGF becomes more visible, their workload and the strategic relevance of the role they play will increase. To ensure that the IGF Secretariat, ideally through the Executive Coordinator, receives the necessary strategic advice and support, we recommend the establishment of a small body made up of members of the MAG and the Leadership Panel to provide advice and support to the UN DESA and the IGF secretariat on organizational matters, including multiyear strategic planning, and monitoring and evaluation of outputs, outcomes and, from time to time, impact.

Rather than an approach whereby the IGF is challenged to "improve" to be relevant, its existing relevance should be recognized and enhanced.

Formalize the role of the IGF in the Roadmap implementation process. The Roadmap implementation has a broad scope and the team responsible for coordinating it should be commended for bringing a wide variety of actors, including from within the UN system, into the process. However, it would be economical in terms of time and financial resources for this process to work with the IGF ecosystem more systematically. Many of the champions and key constituents (concepts used in the Roadmap process) are also active in the IGF. Closer collaboration would rationalize efforts, and allocate responsibility and follow up strategically. Where there is a need for additional institutional capacity to coordinate Roadmap implementation, building this into the IGF plus should be considered before parallel processes are initiated elsewhere. In other words, rather than an ap-

proach whereby the IGF is challenged to "improve" to be relevant, its existing relevance should be recognized and enhanced through using IGF processes actively in coordination with Roadmap implementation.

Harmonize Roadmap and Common Agenda follow-up with WSIS follow-up and implementation. The ITU, working with other UN agencies such as UNESCO, continues to oversee follow-up on the WSIS action lines. There is extensive overlap between the WSIS goals and the Roadmap, as well as with aspects of the Common Agenda. It would enable participation and optimal utilization of resources for these processes to work collaboratively in a more harmonized manner.

Use the IGF as the leading consultation and participation platform for the 7th commitment in "Our Common Agenda." The IGF ecosystem has the credibility and reach across stakeholder groups around the world needed to do the consultation to develop a "Global Digital Compact" in a participative and inclusive manner. This would also provide an opportunity for the IGF to build its capacity to interact more deliberately, on a sustained basis, with decision-making institutions, including national governments. We are not, by any means, suggesting that the IGF should be the sole entity involved in this process. What we propose is that it should be the central platform for facilitating broad engagement and for channelling this into the process of building awareness of the Global Digital Compact and gathering input to go into its drafting.

Maintain the IGF's bottom-up character and continue to maximize its inclusiveness of individuals, but also of institutions. There is a risk reflected to some extent in the terms of reference of the IGF Leadership panel for it to focus on the "high-level" components of the IGF where CEOs, governments, and high-profile individuals from all stakeholder groups get to speak. These spaces are important, but privileging them over the community-organized sessions comes with the risk of overlooking the insights and the concerns of stakeholders "closer to the ground." A high-level layer cannot substitute for building sustainable relationships with decision-making institutions, including governments. That capacity has to also reside in the Secretariat and be available to the MAG.

> As the web of governance grows more complex, there is a natural tendency toward specialization, which can lead to a myopic focus on just a small subset of stakeholders. Making policy is no easy task, and with countless policy development processes taking place around the world, participants in those processes simply end up working in their own silos, unaware of how their outcomes could affect the global Internet, other users, or even their own stakeholders. It's here that the IGF can play an important role. A venue for building shared understanding, awareness of what other governance activities and initiatives are ongoing, and what lessons have been learned is precisely what is needed. A chance for stakeholders in government and national authorities to meet not only with each other, but with the organizations whose focus is on maintaining the global nature of the Internet.[63]

Navigating the IGF for it to remain relevant, and to play the role outlined by Chris Buckridge, above, does not mean navigating the IGF to a safe haven; on the contrary, it means navigating the IGF to the center of the current where it can serve as an inter-disciplinary platform for stakeholders—from the global North and the global South, from government business, the research and academic community, civil society and the technical community—to discuss the diverse and growing range of policy questions pertaining to the Internet.

The IGF is a forum where all participants have some degree of agency, but, when it comes to establishing who is responsible and accountable for its longer-term strength and impact, there is a distinct vacuum. For the IGF to effectively respond to calls for it to grow, to change, and to remain relevant, there is a need to strengthen its organizational and leadership structure. It needs sufficient institutional capacity, funding and leadership to be able to effectively navigate its own growth and development and to maintain a clear presence in the broader Internet governance ecosystem. Clarity on its status and on relationships inside the UN system is also needed to create realistic expectations and lower the threshold for partners from within the UN system to fully participate and to make use of the discussions at the IGF.

For the IGF to effectively respond to calls for it to grow, to change, and to remain relevant, there is a need to strengthen its organizational and leadership structure.

The landscape of Internet governance as a concept, a discipline, and a set of diverse processes evolves constantly. The IGF has to position itself as the one, known, trusted space for those who wish to engage, discuss, and learn, that traverses this shifting Internet governance landscape. A place where there is a comfortable seat and safe space for everyone who cares about, and is affected by Internet-related policy, to say their piece, argue and disagree if needed, and thereby better grasp one another's perspectives, and strive for solutions. This implies having to maintain a delicate balance between, on the one hand, staying the same—such that the IGF is where one can meet old friends and colleagues, and rekindle old debates—and, on the other hand, changing, taking risks, opening up to new and different voices and interests, and interrogating the status quo, but not at the expense of remaining relevant to people and institutions from across the political and stakeholder spectrum.

Endnotes

1 UN Secretary-General, "OUR COMMON AGENDA. Report of the Secretary-General," United Nations, 2021. https://www.un.org/en/content/common-agenda-report/assets/pdf/Common_Agenda_Report_English.pdf

2 The IGF is currently in its third mandate. After two five-year mandates, the IGF mandate was renewed for ten years in 2015 at the ten-year review of the WSIS.

3 According to data from the International Telecommunications Union, 50% of the world population (around 4 billion) used the Internet at the end of 2019. Other sources, such as "Internet World Stats," puts the mid-2021 figure at well over 4.5 billion. See International Telecommunication Union – Development Sector, "Measuring Digital Development: Facts and figures 2020," ITU Publications, 2020, https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2020.pdf

4 World Summit on the Information Security, "Tunis Agenda for the Information Security", ITU, November 18, 2015, Art 72, https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html

5 The Tunis Agenda identifies the main stakeholder groups as being governments, intergovernmental organizations, the private sector and civil society. Later, an understanding of this approache evolved to also include the academic and technical communities as a key stakeholder group.

6 Markus Kummer, "From Tunis to Sharm El Sheikh – The Role of the IGF," Telos – Fundacion Telefonica, https://telos.fundaciontelefonica.com/archivo/numero080/from-tunis-to-sharm-el-sheikh-the-role-of-the-igf/

7 Aside from overall growth in the number of participants, indicators of demand are the large numbers of applications for workshops and other sessions, including from an increased number of institutions and processes applying to the "open forum" format at the IGF to present and discuss their work. There has also been a growing number of first-time participants every year. In 2020, 59% of the 6,150 registered participants attended the IGF for the first time. "IGF 2020 Participation and Programme Statistics," IGF, https://www.intgovforum.org/en/content/igf-2020-participation-and-programme-statistics. In 2019, for the Berlin IGF, 53% of 3,679 participated were first-timers, "IGF 2019 Participation and Programme Statistics," IGF, https://www.intgovforum.org/en/content/igf-2019-participation-and-programme-statistics

8 Open Consultations are typically organized two or three times per year, in conjunction with MAG face-to-face meetings.

9 Aspects of the IGF process can be attributed to the influence of meetings of technical community organizations, particularly those of ICANN and the Internet Society.

10 A multistakeholder advisory group (MAG) was established by the Secretary-General to advise on the program content and schedule of the IGF meetings. The term "Multistakeholder Advisory Group" was only coined a few years into the IGF process. Initially, they were just referred to as the IGF Advisory Group. MAG Terms of reference available at "MAG Terms of Reference," IGF, https://www.intgovforum.org/en/content/mag-terms-of-reference

11 The core of the IGF's organizational structure is the IGF Secretariat, which is located in Geneva but operating under the oversight of the Under-Secretary-General (USG) of the UN Division for Social and Economic Affairs (UN DESA) based at the UN headquarters in New York. This lightweight and decentralized structure is funded through extra-budgetary contributions from entities from all stakeholder groups.

12 Examples of changes introduced in response to the community range from opening up the topics discussed at the forum to providing support for newcomers and adding shorter session formats. In 2011, a "high-level leaders" track was introduced, creating a space for senior officials from governments and other stakeholder groups to engage in interactive discussion on IGF-related topics. A parliamentarian track was introduced in 2019 and "policy networks," designed to make recommendations, in 2021.

13 The latter prefer either an existing institution such as the International Telecommunications Union (ITU) or a new UN office or entity to be as the place to deal with Internet-related matters. An example is the proposal made by India to the UN 66th Session of the UN Annual General Assembly for the establishment of a United Nations Committee for Internet-Related Policies (CIRP). https://cis-india.org/Internet-governance/blog/india-statement-un-cirp

14 United Nations General Assembly and Economic and Social Council, "Report of the Working Group on Improvements to the Internet Governance Forum," A/6765-E/2012/48, United Nations, March 16, 2012, https://unctad.org/system/files/official-document/a67d65_en.pdf

15 The report also addressed IGF processes such as the nomination of MAG members, emphasizing the need for transparency. Even though there were still only a handful at the time, it also encouraged stronger interconnection with regional IGFs.

16 IGF, "IGF Retreat. Advancing the 10-Year Mandate of the Internet Governance Forum, Summaries" IGF, July 2016, http://www.intgovforum.org/cms/documents/igf-meeting/igf-2016/812-igf-retreat-proceedings-22july/file

17 The mandate was extended for a further ten years at the end of 2015.

18 The MAG Working Group on IGF Strategy and Strengthening in the course of 2020 concluded that most of the recommendations made by the CSTD working group and the IGF retreat had not been implemented fully. MAG Working Group on IGF Strengthening and Strategy, "Unpublished Background document: Analysis of previous recommendations on Improvements to the IGF," IGF, August 2020, https://www.intgovforum.org/en/filedepot_download/10447/2388

19 UN Secretary General, "Secretary-General's Roadmap for Digital Cooperation," United Nations, June 2020, https://www.un.org/en/content/digital-cooperation-roadmap/

20 "Roadmap on Digital Cooperation Key Action Areas as outlined on the website—One, Achieving universal connectivity by 2030; Two, Promoting digital public goods to create a more equitable world; Three, Ensuring digital inclusion for all, including the most vulnerable; Four, Strengthening digital capacity-building; Five, Ensuring the protection of human rights in the digital era; Six, Supporting global cooperation on artificial intelligence; Seven, Promoting trust and security in the digital environment; Eight, Building a more effective architecture for digital cooperation." The report itself follows a different structure but the ideas are consistent across the site and the full document.

21 Paragraph 67 of the Roadmap. UN Secretary-General, "Report of the Secretary-General. Roadmap for Digital Cooperation," United Nations, June 2020, https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf

22 In chapter four, "Mechanisms for global digital cooperation," an IGF-plus is one of three proposed mechanisms. UN Secretary-General's High Level Panel on Digital Cooperation, "the age of digital interdependence," United Nations, https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf

23 The Roadmap recognizes that different digital architecture models proposed by the HLP-DC are still under discussion, but clearly highlights ideas that have emerged to make the IGF "more responsive and relevant to current digital issues."

24 "Consultation on the follow-up on the UN Secretary-General's High-Level Panel on Digital Cooperation convened by the MAG Chair supported by the Government of Switzerland," IGF, January 14, 2020, https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/9615/1986 .

25 Submissions made by various parts of the IGF ecosystem, from national, regional, and youth IGF initiatives, (NRIs) to Best Practice Forums and from many institutions in the broader IGF community, in response to the above-mentioned January 2020 IGF Open Consultation, echo and welcome the idea of a strengthened IGF that also maintains its essential "bottom-up" character.

26 "MAG Chair Activities", IGF, https://www.intgovforum.org/en/content/mag-chair-activities

27 "IGF 2020. Reviewing past BPFs to enhance future BPF work: a "BPF on BPFs," IGF, September 2020, https://www.intgovforum.org/en/filedepot_download/3405/2212

28 A learning study on Best Practice Forums produced a report and recommendations in 2020, and a similar study on Dynamic Coalition will be published in November 2021.

29 In their capacity of co-champions for following up on recommendations 5A/B on the architecture for digital cooperation in the report of the UN Secretary-General's HLPDC.

30 Germany and the United Arab Emirates, "The Options Paper," Global Cooperation, September 3, 2020, https://www.global-cooperation.digital/GCD/Navigation/EN/The-Options-Paper/the-options-paper.html

31 Germany and the United Arab Emirates, "The Options Paper," Global Cooperation, September 3, 2020, https://www.global-cooperation.digital/GCD/Navigation/EN/The-Options-Paper/the-options-paper.html

32 "IGF Main Session on Internet Governance & Digital Cooperation," IGF, November 26, 2019, https://www.global-cooperation.digital/GCD/Redaktion/EN/Downloads/igf-main-session-on-Internet-governance.pdf?__blob=publicationFile&v=2

33 Report of the First IGF 2020 Open Consultations submitted as input for the Options paper. "First IGF 2020 Open Consultations and Multistakeholder Advisory Group (MAG) Meeting United Nations Office at Geneva (UNOG)," IGF, January 14, 2020, https://www.global-cooperation.digital/GCD/Redaktion/EN/Downloads/contribution-geneva-multistakeholder-advisory-group.pdf?__blob=publicationFile&v=2

34 "IGF 2020 Main Session: Digital Cooperation," IGF, November 12, 2020, https://www.intgovforum.org/en/content/igf-2020-main-session-digital-cooperation

35 This was also not a new idea. The previous MAG chair initiated a MAG working group on multi-year planning in 2018.

36 MAG Working Group on IGF Strengthening and Strategy, "MAG Working Group on IGF Strengthening and Strategy (WG-strategy) proposals on strategic improvements to the IGF and operational measures in 2021," IGF, January 22, 2021. https://www.intgovforum.org/en/filedepot_download/10447/2458

37 Internet Governance Forum Multistakeholder Advisory Group Working Group, "Internet Governance Forum Multistakeholder Advisory Group Working Group on IGF Strategy and Strengthening, 2020: Response to the paper on 'Options for the Future of Digital Cooperation'," IGF, September 29, 2020. https://www.intgovforum.org/en/filedepot_download/10447/2267

38 UN Secretary-General's High Level Panel on Digital Cooperation, "the age of digital interdependence," United Nations, p.24 https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf

39 Early in 2021, the Secretariat initiated a consultation to gain further input on the proposed Multistakeholder High-level Body (MHLB). They received 85 submissions in response, but at the time of writing the future form and terms of reference of this body were not yet known. The list of inputs received in response to the consultations on paragraph 93(a) in the Roadmap for digital cooperation, https://www.intgovforum.org/en/93a-public-responses

40 "INTERNET GOVERNANCE FORUM LEADERSHIP PANEL - Call for Nominations," IGF, https://www.intgovforum.org/en/content/internet-governance-forum-leadership-panel-call-for-nominations

41 The Leadership Panel will include two ministerial-level or above representatives from Governments that are Member States of the United Nations or regional intergovernmental organizations that have observer status in the General Assembly; two CEO-level (or deputy-level) representatives from each of the other three stakeholder groups (private sector, technical community, and civil society) and two at-large members (distinguished or prominent persons who do not fall under the above stakeholder groups). Ex-officio members will include three senior representatives (Minister or head of agency-level) made up of the current, immediately previous, and the immediately upcoming host countries, the Chair of the IGF's Multistakeholder Advisory Group (MAG), and The Secretary-General's Envoy on Technology.

42 "Terms of Reference for the IGF Leadership Panel," IGF, https://www.intgovforum.org/en/content/terms-of-reference-for-the-igf-leadership-panel

43 "Terms of Reference for the IGF Leadership Panel," IGF, https://www.intgovforum.org/en/content/terms-of-reference-for-the-igf-leadership-panel

44 "United Nations. Office of the Secretary-General's Envoy on Technology," United Nations, https://www.un.org/techenvoy/

45 This followed up on a recommendation in the report of the Secretary General's High-Level Panel on Digital Cooperation: UN Secretary-General's High Level Panel on Digital Cooperation, "the age of digital interdependence," United Nations, https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf

46 "About the Office of the Secretary-General's Envoy on Technology," United Nations, https://www.un.org/techenvoy/ (accessed 16 Nov 2021).

47 With regard to the architecture for digital cooperation, their website states that "In line with the key recommendations of the Roadmap, discussions are ongoing, including with the IGF community and efforts underway to strengthen the IGF. On this, the Office works closely with the UN DESA," "Building a more effective architecture for digital cooperation," United Nations, https://www.un.org/techenvoy/content/global-digital-cooperation (accessed 16 Nov 2021)

48 UN Secretary-General, "OUR COMMON AGENDA. Report of the Secretary-General," United Nations, 2021. https://www.un.org/en/content/common-agenda-report/assets/pdf/Common_Agenda_Report_English.pdf

49 UN Secretary-General, "OUR COMMON AGENDA. Report of the Secretary-General," United Nations, 2021, p. 83, paragraph 131. https://www.un.org/en/content/common-agenda-report/assets/pdf/Common_Agenda_Report_English.pdf

50 The 12 commitments can be found on page 7 of "Our Common Agenda." UN Secretary-General, "OUR COMMON AGENDA. Report of the Secretary-General," United Nations, 2021, p.7. https://www.un.org/en/content/common-agenda-report/assets/pdf/Common_Agenda_Report_English.pdf

51 UN Secretary-General, "OUR COMMON AGENDA. Report of the Secretary-General," United Nations, 2021, p.63, paragraph 93. https://www.un.org/en/content/common-agenda-report/assets/pdf/Common_Agenda_Report_English.pdf

52 Included in the Common Agenda, under "Improve Digital Cooperation", the 7th of the 12 commitments. UN Secretary-General, "OUR COMMON AGENDA. Report of the Secretary-General," United Nations, 2021. https://www.un.org/en/content/common-agenda-report/assets/pdf/Common_Agenda_Report_English.pdf

53 Ibid.

54 Ibid.

55 UN Secretary-General, "Report of the Secretary-General. Roadmap for Digital Cooperation," United Nations, June 2020, paragraph 93 https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf

56 Ibid., paragraph 93 (g).

57 From 2011 onward for a few years, the IGF Secretariat did not have senior leadership at all, until eventually Mr. Chengetai Masango, IGF Programme and Technology Manager, became established as the Head of Office of the Secretariat. He is supported by a small team of staff and consultants but he does not have the authority of an Executive Coordinator.
The IGF Secretariat in October 2021, "Team", IGF, https://www.intgovforum.org/en/about#team

58 From 2005 to 2010, the IGF Secretariat was led by an Executive Coordinator, Mr. Markus Kummer, who had also led the Working Group on Internet Governance (the group mandated by the UN Secretary General to develop recommendations on the future of Internet governance in the period between the two phases of the World Summit on the Information Society.

59 When the advisory group that later became known as the MAG was first convened in 2006,

it was chaired by Nitin Desai, at that time a retired Under Secretary-General of the UN, in his capacity as Special Advisor to the UN Secretary-General. Nitin Desai's presence contributed significantly to the legitimacy of the IGF in two respects: it provided a high-level link to the United Nations as an institution, and in particular to the UN Secretary-General, and it contributed to maintaining a global-South perspective and development-oriented focus. After Nitin's retirement, the position of IGF "Special Advisor" remained vacant, in spite of frequent calls from all stakeholder groups for it to be filled.

60 World Summit on the Information Security, "Tunis Agenda for the Information Security", ITU, November 18, 2015, paragraph 72, https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html

61 The mandate also asks the IGF to: "Facilitate the exchange of information and best practices, and in this regard make full use of the expertise of the academic, scientific, and technical communities; advise all stakeholders in proposing ways and means to accelerate the availability and affordability of the Internet in the developing world; strengthen and enhance the engagement of stakeholders in existing and/or future Internet governance mechanisms, particularly those from developing countries; identify emerging issues, bring them to the attention of the relevant bodies and the general public, and, where appropriate, make recommendations; contribute to capacity building for Internet governance in developing countries, drawing fully on local sources of knowledge and expertise; promote and assess, on an ongoing basis, the embodiment of WSIS principles in Internet governance processes; discuss, inter alia, issues relating to critical Internet resources; help to find solutions to the issues arising from the use and misuse of the Internet, of particular concern to everyday users; publish its proceedings," "About Us," IGF, https://www.intgovforum.org/en/about#about-us

62 The Just Net Coalition statement on the MHLB in response to the 2020 consultation convened by the Secretariat reflects this perspective. The Just Net Coalition, "More than 170 Civil Society Groups Worldwide Oppose Plans for a Big Tech Dominated Body for Global Digital Governance," Just Net Coalition, https://justnetcoalition.org/big-tech-governing-big-tech.pdf

63 Chris Buckridge, "Do We Need The IGF? Now More Than Ever!," RIPE Labs, November 2, 2021, https://labs.ripe.net/author/chrisb/do-we-need-the-igf-now-more-than-ever/. Chris Buckridge is advisor to the RIPE NCC managing director on issues of Global Strategic Engagement.

About the Authors

Anriette Esterhuysen is currently the Chair of the Multistakeholder Advisory Group of the United Nations Internet Governance Forum. She was the executive director of the Association for Progressive Communications (APC) from 2000 to 2017. She continues to work with APC on convening the African School on Internet Governance (AfriSIG), a joint initiative of APC, the African Union Commission and Research ICT Africa. Anriettewas inducted into the Internet Hall of Fame as a Global Connecter in 2013 and received the EFF Pioneer award in 2015. She serves as a Commissioner on the Global Commission on the Stability of Cyberspace and is a member of the editorial board of the Journal of Cyber Policy. She serves on the board of .ZADNA, the South Africandomain name authority and Connect Humanity, a new global fund for digital equity.

Wim Degezelle is an independent Internet Policy Analyst and Consultant with over 20 years' experience. A Political scientist by training, he started his career as policy assistant in the European Parliament, but soon moved to Internet policy and governance. His active long-term participation in community-driven forums and organisations such as the United Nations Internet Governance Forum and technical communities like ICANN and CENTR, made him a true believer in the value of the multi-stakeholder policy dialogue to address the many challenges emerging from our growing dependence on digital technologies and the Internet.

Cyberstability Paper Series

New Conditions and Constellations in Cyber

Routing Without Rumor

Securing the Internet's Routing System

Danny McPherson
Executive Vice President & Chief Security Officer, Verisign

Routing Without Rumor: Securing the Internet's Routing System

Danny McPherson | Executive Vice President
& Chief Security Officer, Verisign

The Global Commission on the Stability of Cyberspace (GCSC) has spent a considerable amount of time and resources developing eight norms by which to influence state and non-state behaviors to support the stability of cyberspace.[1] One of these norms focuses on "the public core of the Internet," which at a high level constitutes "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." A more detailed definition of the Norm on the Non-interference with the Public Core[2] is available on the GCSC website.

The Norm declares that "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."

This paper, in the GCSC's "New Conditions and Constellations in Cyber" Cyberstability Paper Series,[3] is primarily concerned with the public core of the Internet's packet routing and forwarding elements, as well as with corresponding Internet numbering systems. We'll first provide some background information on the Internet architecture and Internet number resource allocation, and then discuss some vulnerabilities in the Internet routing system and what mechanisms are aiming to mitigate those vulnerabilities. We'll then provide some considerations all stakeholders need to consider as we aim to find a balance between vital new infrastructure components, such as Resource Public Key Infrastructure (RPKI) that aims to help secure the routing system, and the implications that come along with its adoption.

Danny McPherson is Executive Vice President and Chief Security Officer at Verisign. He has authored several books, numerous internet protocol standards, network and security research papers, and other publications.

The Internet Protocol (IP) and Internet Number Resources

The Internet is made up of a loosely interconnected network of networks. These networks utilize the Internet Protocol (IP) suite, a collection of technical standards and rules, to relay packets within and between networks. IP provides the formatting of data exchanged as well as the addressing system, and a routing function is provided by systems referred to as routers that enables the inter-networking, allowing information to be exchanged between networks and creating a unified single global network—the Internet.

IP addresses are used to uniquely identify each device on the Internet. There are two types of IP addresses used on the Internet today: the 32-bit IP version 4 (IPv4) addresses, which allow for unique addresses of just over ~4 billion endpoints (232), which seemed sufficient when the Internet was first developed, and a newer version of IP, the 128-bit IP version 6 (IPv6) addresses, which provides ~340 undecillion (2128) of available addresses.

Just as with phone numbers, global uniqueness of IP addresses for devices connected to the Internet is crucial. To maintain uniqueness of IP addresses, global coordination and allocation is required. As illustrated in Figure 1, IP addresses are distributed in blocks (i.e., address ranges) from the Internet Assigned Numbers Authority (IANA) to the five Regional Internet Registries (RIRs), who assign them to National Internet Registries (NIRs), Local Internet Registries (LIRs), or directly to Internet Service Providers (ISPs) and end users.[4]

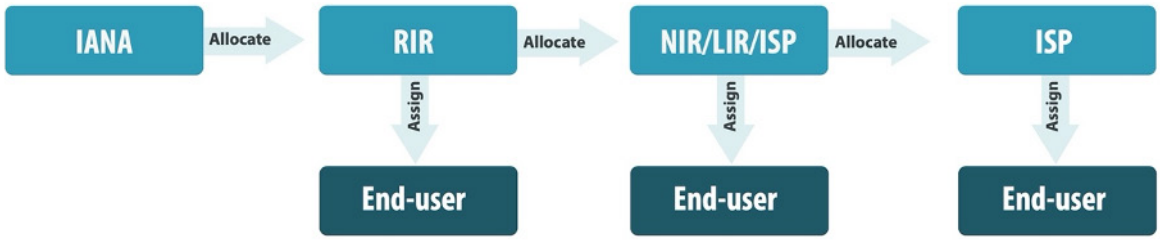


Figure 1: Internet Number Resource Allocation: IP Addresses and AS Numbers (source: ARIN.net)

In addition to IP addresses, each network that connects to the Internet needs to obtain a unique Autonomous System (AS) number, which is used by routing protocols to identify that network within the global routing system. These AS numbers are distributed in the same manner as IP addresses. AS numbers were originally specified as 16-bits, allowing for AS numbers from 0 through 65535. In the mid-2000s the Internet Engineering Task Force (IETF)[5] developed backwards-compatible 32-bit AS numbers (~4 billion) and transitioned to the larger AS numbers. Today, AS numbers are allocated from this larger number space, and it's a good thing, given that there are already ~72,500 unique ASes represented in the global routing system currently.[6]

The collection of network devices, border and internal routers that comprise each network connected to the Internet vary considerably. For example, a small enterprise may only have one low-end internal and Internet-connect router, whereas a large enterprise, regional ISP, or university may have hundreds or thousands, and a large ISP may have thousands or even tens of thousands of routers.

Similarly, where these networks connect to the Internet will vary. Small enterprises may only connect in one location to a regional or local ISP, whereas large enterprises may connect in tens or

hundreds of locations, and interconnect with other networks either directly or at one or more Internet Exchange Points (IXPs).[7] Large ISPs may interconnect with other networks in multiple locations and across many regions and countries, as well as via a multitude of IXPs. Regardless of where and how they interconnect, if they're connecting to and participating in the global routing system, they'll generally use a single AS number to uniquely identify their network. Each individual network is designed to support the business and policy objectives of that individual network's administrators. There is no centralized planning authority or coordination facility dictating how or where networks interconnect globally.

Correspondingly, the number of network administrators will vary considerably, where there may be only one or two at a small network, but potentially hundreds at a large ISP. In aggregate, there may be a million or more individuals involved with routing on the global Internet.

Internet Routing and the Border Gateway Protocol (BGP)

Networks often interconnect at a multitude of locations. The primary job of the routing system is to learn all available paths through the network(s) to reach a particular destination, and when faced with a multitude of paths for a given route, to use what local administrators deem as the best route at any given instant. In the routing system, these destinations are codified as blocks of IP addresses, commonly referred to as prefixes (much like the telephone numbering system), and metadata is added to the prefix identifying the network(s) the information traversed within the routing system to reach the local router. This prefix and associated metadata constitute what's referred to as destination network layer reachability information, or a "route." Routes can be for either IPv4 or IPv6 destinations, and there are ~903,000 IPv4 prefixes in the current routing system, and ~142,000 IPv6 prefixes.[8]

Time and again, the Internet routing system has proven to be highly effective and robust in the face of localized and regional failures, finding alternative available routes to a destination if the current preferred route becomes unavailable. The global routing system has dealt with immense scaling challenges across multiple dimensions (e.g., the number of ASes, the number of discrete interconnections, the growth of routes, the number of available paths to reach a given destination, and the amount of instability or "churn" in the system).

Today, the routing system largely relies on a decentralized and implicit trust model of network self-assertions that effectively creates a transitive "web of trust." There is no central authority dictating which networks are authorized to assert reachability for an Internet destination.

The Border Gateway Protocol (BGP),[9] standardized by the IETF, is the de-facto inter-domain routing protocol on the Internet. Conceptually, border routers within each AS establish BGP peering sessions internally, as well as across each point of interconnection with border routers in other ASes, and the routers are referred to as BGP neighbors, as illustrated in Figure 2. In accordance with local routing policies, each router advertises destination reachability information to each of their BGP neighbors, effectively self-asserting that they provide reachability to the collections of IP addresses within the IP address block(s) represented by the route(s). It is these routing policies that therefore decide where and how Internet traffic flows, which not only factors into account performance characteristics, such as availability and latency, but also potentially the security of resulting data that will be transmitted, as well as the financial cost of exchanging data in certain locations. Understanding how routing works is therefore a major factor in understanding both Internet security and Internet economics.

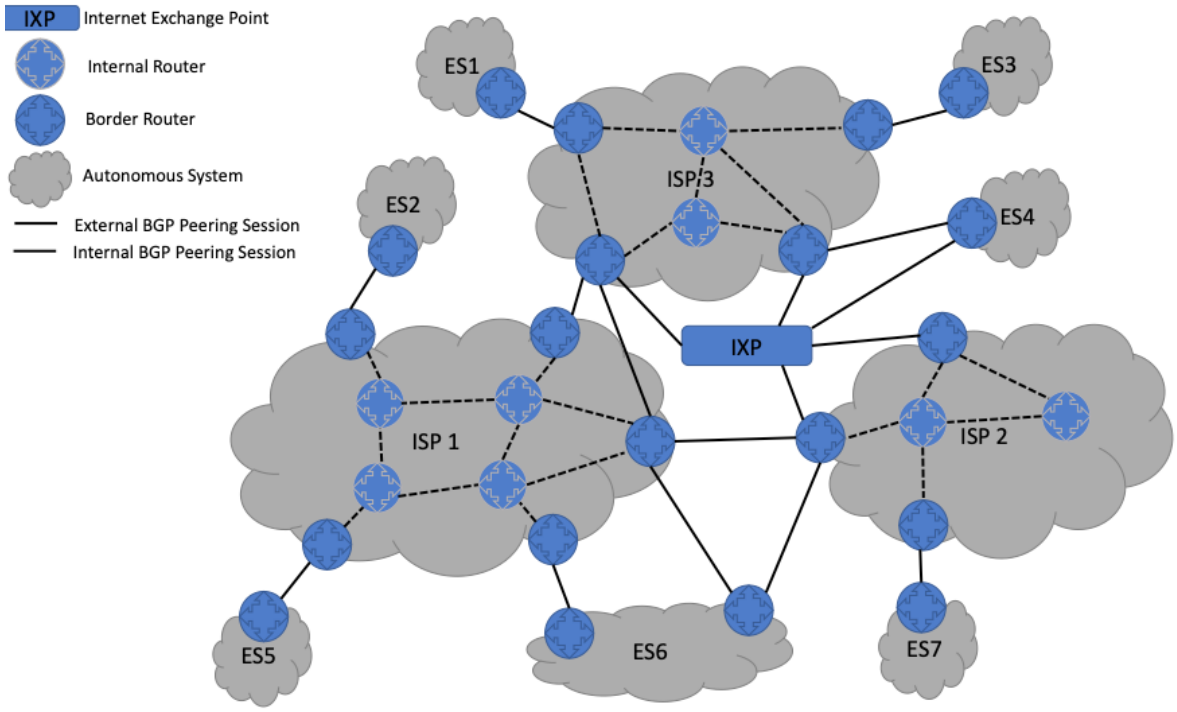


Figure 2: Sample Inter-domain Interconnection Model

Today, the routing system largely relies on a decentralized and implicit trust model of network self-assertions that effectively creates a transitive "web of trust." There is no central authority dictating which networks are authorized to assert reachability for an Internet destination. Each individual AS independently applies its own locally provisioned policies, choosing what action to take on each of the destinations for which it locally provides connectivity, as well as on all of the routes it received from other networks. For each route received from a peer, a router may choose to

1. only use the information locally for packet forwarding (e.g., in Figure 2 if ISP1 were to receive a route for a destination connected to End Site 4 (ES4) from ISP3, they might choose to only share it with end sites (customers) connected to them, and not with ISP2, or
2. use the information locally as the preferred route and propagate it (i.e., advertise destination reachability) to one or more of its peer networks, to include ISP2, which could result in ISP1 being in the datapath for the route if ISP2 has no other route, or
3. simply discard or suppress the route received from the peer and not share it with anyone.

When a preferred route to a destination learned via a given path (e.g., internally or via a BGP neighbor in another AS, as illustrated in Figure 2) becomes unavailable, and if an alternative path via another router exists, the alternative can immediately be used to reprogram the router's packet forwarding logic and the router can continue to transmit traffic toward the destination. This may result in a less desirable path being used, e.g., in action 3 above where traffic may flow from ISP2 through ISP1 to get to ISP3 and ultimately, ES4 if the IXP were to become unavailable.

Despite being designed over three decades ago in a vastly different Internet, BGP has scaled so well because (a) it operates in a distributed manner, (b) it has no central point of control and therefore of failure, and (c) each network acts autonomously with regard to whom it interconnects with

and what information it chooses to use and/or propagate. While an array of pricing, performance, and security characteristics are used to develop routing policies in each AS, ultimately BGP will use any available path to reach a destination, and often enough the choice of how to route between two ASes is dependent upon interpersonal factors between the individual network administrators themselves, and upon informal assessments of technical and even personal reliability—this behavior could be considered routing by rumor. In the idealized scenario where network operators only deal with noble actors, and none of the million(s) of network administrators are capable of mistakes, and there is zero probability that bad actors would gain access to one or more of those networks, then this distributed system would function well and could be fully trusted. But pragmatically in today's world, where routing incidents continue to cause operational and security issues, operators know the idealized scenario is not the case. Much like the Domain Name System (DNS) and other early Internet infrastructure protocols in which ease of use, open end-to-end connectivity, system resilience, and scalability were primary objectives, security was an afterthought.

Much like the Domain Name System (DNS) and other early Internet infrastructure protocols in which ease of use, open end-to-end connectivity, system resilience, and scalability were primary objectives, security was an afterthought.

Routing Security Incidents

The two most prominent types of operational and security incidents that occur in the routing system today are "route hijacks"[10] and "route leaks."[11] Route hijacks involve the accidental or malicious rerouting of internet traffic and are sometimes referred to as mis-origination,[12] in which the originating AS contained within the BGP metadata associated with the route is usually not the legitimate origin. Route leaks typically involve the unintentional or malicious propagation of routing information beyond the intended scope of the originator, receiver, and/or one of the networks along the route's path, thereby resulting in potentially unintended or undesirable networks being inserted into the datapath used to reach a given destination. For example, imagine a scenario where ES6 in Figure 2 began announcing to ISP2 routes that it had learned from ISP1, and because routing policies commonly prefer customer-learned routes over peer-learned routes, traffic from ISP2 to ISP1 destinations begins flowing through ES6. As a result, there could be latency and packet loss issues, as well as potential man-in-the-middle (MitM) or denial of service attack conditions as a result.

Often, route leaks will preserve the originating AS in the route's metadata, but that's not always the case. Interestingly, if the origin is preserved during a route leak, then many of the origin validation controls that may be in place are implicitly circumvented. Both route hijacks (e.g., how Pakistan Telecom effectively globally exported their state censorship on YouTube services[13]) and route leaks[14] can result in partial or full rerouting of traffic for the impacted destinations. This can potentially result in changes to the packet forwarding path and have an array of security implications. These include enabling denial of service conditions, when traffic is selective or discarded wholesale either intentionally or because of insufficient resources to forward it on to the intended destination. It can also facilitate man in the middle (MitM) and Man-on-the-Side, and other "on-path" attacks, which can allow an attacker the opportunity with which to influence the confidentiality, availability, and even integrity of the data stream, depending on the attacker's sophistication and the type of encryption used. Not all the incidents are intentional. However, discerning intent is extremely difficult given that the complexity of routing policy configuration, deployment, and implementation vary considerably.

Some routing incidents may also simply be a misconfiguration that results in added latency, and/or potential network congestion, in reaching the destination without attack exposure. Leaks occur very frequently in the routing system[15] and it's often difficult to ascertain if the cause is due to a mistake or malice, but regardless, the immediate effect is usually the same. Therefore, individual presumptions on the reliability of an operator and subjective assessments if an incident is accidental or intentional are not only a regular feature, but a key aspect of routing security.

Solving the problem of BGP insecurity to prevent future route hijacks and even route leaks requires considerable coordination in the Internet community, a concept that fundamentally goes against the distributed action and autonomous operations design tenets of BGP. Once an ISP or end site receives an internet address block and an AS number allocation from its Regional Internet Registry (RIR),[16] typically, it would need to register specific information to include the local "origin AS" / IP address block (prefix) associations in one or more Internet Routing Registries (IRRs)[17] so that their ISPs and potentially other networks can generate routing policies and "filters" in accordance with local policies. Furthermore, each network may be required by its ISP to publish routing policies regarding what upstream networks (ASes) are authorized to provide "transit services (e.g., an ISP providing an enterprise global connectivity) for the network's destinations (i.e., authorized upstream peers). Requirements for publication of this information in one or more IRRs is voluntary and is solely up to each individual AS, some of which may proxy register routes in IRRs for their customers, utilize alternative internal customer configuration and routing policy databases, or perhaps not require any route registration at all. A key characteristic of the BGP system is that any AS can potentially announce reachability for any IP addresses to the entire world, meaning that any single AS can potentially have a detrimental effect on the global reachability of any Internet destination.

For instance, if the routing information is published in an IRR, other non-adjacent network operators may also use that information to provision routing policies in their routers. The complexity of computing IRR-derived filters for each feasible path to reach a given destination can be considerable for large network operators, especially as new networks and network interconnections are added and as one moves closer to the largest "tier-1" networks at the core of the Internet, where even the largest routers today can't load policy information for all the feasible paths reachable via each of its BGP neighbors. Routing policies may specify whether to accept one or more specific routes from one or more peers and/or customers, and, with a specific origin AS, from a particular peer that has been authorized to announce the route.

RFC 7682[18] outlines some of the historical and existing challenges with the IRR model. The most significant of these challenges is that there are a multitude of IRRs in operation,[19] some operated by ISPs, some operated by research and academic institutions, some by RIRs,[20] and some by for-profit entities. With a few exceptions (e.g., RIPE IRR[21]), there is little to no strict tethering of who holds what number resources with who is authorized to publish routing information for those number resources in any given IRR. As a result, bad actors, misconfigurations, automated proxy registrations by ISPs, or other errors have resulted in a large amount of information being published in IRRs that may not be reliable for provisioning of inter-domain routing policies and may even cause unintended scaling or security issues. Furthermore, the data stored and provided by IRRs is not cryptographically verifiable by relying parties, and stale information is rarely purged from the IRR system. Despite these shortcomings, most inter-domain routing policies today are still provisioned based on the IRR system.

The Resource Public Key Infrastructure (RPKI)

Fortunately, there is a solution already available and gaining considerable deployment traction. A new system, primarily supported by the five RIRs,[22] is referred to as Resource PKI (RPKI) and provides a cryptographic number resource certification infrastructure. The RPKI enables Internet number allocation authorities and resource holders (e.g., ISPs and end sites) to specify "Route Origin Authorizations (ROAs)" that are cryptographically verifiable and can be used by relying parties (i.e., network operators) for ingesting route origin verification data. That data can be used to automate ingestion of data and configuration of origin validation routing policies directly into routers, automating much of what were historically cumbersome workloads that were prone to operational issues and configuration "drift," and complex for even the most sophisticated routers to process. This nascent RPKI system was developed in the IETF and is standards-based. The RPKI does appear to be gaining traction[23,24] and will certainly address many of the issues that led to decay of various sorts with the current IRR system. Furthermore, it could also be used to bootstrap or otherwise inform and revitalize the IRRs, allowing network operators to identify what information in an IRR was derived from the RPKI and which can therefore be cryptographically validated and associated with routing policies.

The RPKI does appear to be gaining traction, and will certainly address many of the issues that led to decay of various sorts with the current IRR system.

RPKI brings a new set of challenges of its own. Foremost, RPKI creates new external and third-party dependencies that, as adoption continues, ultimately challenge the autonomous operations of the routing system and, if too tightly coupled to the routing system, may impact the robustness and resilience of the Internet itself. RPKI relies on the DNS, and the DNS depends on the routing system. Therefore, particular attention needs to be paid to these interdependencies. Specifically, with RPKI, network operators need to be careful not to introduce tightly coupled circular dependences where the routing system in turn relies on the RPKI, especially at times of startup and instability, otherwise recovering from instability and outages could result in race conditions (i.e., where a system tries to perform multiple functions in parallel that need to be done in sequence[25]) or other bootstrapping issues. This threat can be avoided by ensuring proper operational buffers are in place to absorb failures to various components of the system. A great deal of research has been done considering systemic dependencies and their implications on communications resilience (e.g., the NSTAC Report to the President on Communications Resiliency[26]), and the RPKI system itself would certainly fall into this category of "public core of the Internet" and should be factored into account accordingly.

Perhaps the most significant challenge to RPKI is how the activities of the RIRs can potentially have direct operational implications on the routing system. Unlike the DNS, the global RPKI as deployed does not cleanly model the number resource allocation hierarchy and does not have a single root. Instead, it has multiple trust anchors, operated by each of the RIRs. Currently, the RIRs "over-claim" number resources[27,28,29] to ease complexity of number resource transfers between RIRs.[30] This effectively puts the onus on the relying parties (i.e., network operators)[31] to resolve conflicts should they occur, whereas those relying parties have little to no capability to resolve such conflicts (i.e., how could they know which of two remote ASes that received number resources from different RIRs is the authorized entity to originate a given route?). It also means that a compromise of any RIR's RPKI infrastructure could potentially impact the entire system—regardless of from where a number resource was assigned. While one potential mitigating control is for RIRs to greatly increase the security and stability of their RPKI infrastructure, they'll still be prone to attacks and operational errors alike. If the RIRs were to refrain from overclaiming number resources (and address

the transfer issues via other means), then operators would need to worry primarily about their RIR as far as routing of the prefixes they originate goes. Each Operator would need to interface with all of the RPKI infrastructure when they develop and generate their own routing policies. Even then, a fully operational RPKI that's used to develop routing policy by network operators more broadly will require the RIRs to develop and maintain levels of security and 24x7 operations for which they've traditionally not been funded or required to provide,[32] a growing pain their members are surely going to need to fund in the coming years.

While a cryptographically verifiable number resource allocation repository is a necessity for securing the routing system,[33] just how loosely or tightly coupled that system is to the current Internet routing system will ultimately determine the fragility of the system, and the ability for entities of that system to preserve necessary autonomy in operations. Furthermore, by the very nature of bolting a hierarchical system on to a loosely distributed routing system, the RPKI itself potentially introduces new control points (e.g., the RIRs themselves) and security vulnerabilities. These include so-called "grandparenting" attacks (where someone in the allocation hierarchy takes an action undesirable to the resource holder)[34] and other attacks that may not necessarily exist in the inherently insecure and loosely coupled legacy IRR model, where routing by rumor is the norm. The ideal state is to find a balance between the vital new structure of the RPKI, as well as the inherently ad hoc but tried-and-tested system of routing by rumor.

The collection of systems that makeup the RPKI is very nascent. The scale, stability, and security of the RIR infrastructure that constitute much of the RPKI will play a much more critical role in the operations and security of the routing system in the future than RIR systems have historically played. Traditionally, RIRs allocate Internet number resources (address space and AS numbers) to ISPs or end sites and make available information associated with those allocations via WHOIS[35] or other means. Beyond perhaps operating various components of DNS infrastructure and an IRR themselves, RIRs had no direct operational tie-in to how the number resources are utilized in the routing system. An RPKI-enabled routing system requires constant maintenance, high performance, robust security, and high availability. This is a significant departure from the traditional operational expectations of RIRs. The increased operational importance of RIRs means that they, too, should be considered part of the public core of the Internet.

Given the risks associated with this new role, the RIRs are still evolving their own organizational thinking, from both legal[36] and technical perspectives,[37] and are prudently reminding relying parties to be cautious when coupling the RPKI to their network routing policies[38] without sufficient operational buffers.

With the growing reliance on the Internet for mission-critical functions, and continuing concern about insecurities of the routing system, the promise of RPKI to ameliorate some of the vulnerabilities is being well received, as evidenced by its rate of adoption. RPKI has seen significant growth in adoption over the last three years, from ~10% of registered Prefix-Origin pairs having RPKI validation data at the end of 2018, to ~31% valid Prefix-Origin pairs in October 2021. RPKI adoption percentages are not uniform at each RIR, yet by any measure, they've been impressive.[39]

Beyond the RIRs, a significant number of Tier-1 telecom providers (e.g., GTT, NTT, and Telia[40]) and large network operators have fully implemented RPKI-based origin validation. According to "Is BGP Safe Yet"[41] (which conjectures that RPKI makes it safe), 102 known operators worldwide have completed the full implementation of RPKI. An additional 24 operators have partial RPKI deployment, and another 240 operators have only just begun the process of RPKI deployment. While that

still leaves another ~72,000 networks[42] to act, it is a significant deployment rate in such a relatively short timeframe, especially when compared to historic IPv6 and DNSSEC deployment rates.

The original objective of RPKI-based origin validation was to prevent perhaps the most significant class of notable routing security incidents, those that involve re-origination of routes the local AS is not authorized to announce. Re-origination incidents are commonly the result of router policy misconfiguration or buggy software. The Pakistan / YouTube Incident,[43] in which Pakistan announced YouTube address space globally while attempting to censor it locally within Pakistan, had the effect of taking all of YouTube offline globally. Another similar incident, , commonly referred to as the infamous AS7007 incident,[44] occurred when a BGP router operated by AS7007 accidently announced to the Internet that it was the proper destination AS for a large portion of Internet address space. In these types of incidents, mis-origination was easily identifiable. The impact with these and similar incidents is commonly compounded when the routing announcements are "more specific" than the legitimate announcements, as IP routing protocols normally always prefer the most specific route over less specific routes.

Without RPKI, a sophisticated attacker can likely circumvent AS origin validation alone quite easily, and it commonly happens even by default with many forms of route leaks, although when it does, it makes intent of the misbehaving network easier to identify. Origin validation, be it based on RPKI or IRR routing policy information, will certainly prevent an entire class of BGP security incidents that occur commonly today.

One final note with RPKI-based origin validation and its IRR-based counterparts, however, is that the manipulation of a BGP AS path, including the origin, is still possible, and until cryptographic security protocols that link RPKI to routing protocol integrity protections can be deployed at scale, this problem will persist. There has been a large amount of additional work to address BGP path validation beyond just the origin via protocols such as BGPsec,[45] where RPKI-derived cryptographic signatures are attached to information within the routing system and BGP itself to provide integrity protections. However, it remains to be seen if this work is worth the complexity and fragility it introduces, especially as it is still vulnerable to route leaks[46] and other similar forms of attack that need to be addressed via peering and operational best practices, as discussed in the next section.

While attacks leveraging the routing system can be targeted and intentionally scoped, most attacks in the routing system are noisy, globally propagated, and fairly trivial to detect. Of course, as discussed previously, discerning whether a given routing security incident was the result of malice or error is complex for external observers. While the immediate effect is often the same, it is common that little to no authoritative information on the root cause for a given incident ever emerges. Fortunately, network operators can take decisive action to filter and "reverse" bad routing information once identified, and the offending network(s) are commonly identified in operational and security forums, but there is often little to no recourse. This noise factor associated with routing system attacks is likely an attribute from where much restraint for launching such attacks stems, for state and non-state actors alike. Yet they still seem to have occurred,[47,48,49,50] and likely will continue to occur, and even if only temporary, it's important to recognize that the attacker's objective may have been achieved. As with most security, this is where layered defenses and best practices come into play, as discussed in the following section.

Beyond the supporting infrastructure mechanisms (e.g., RPKI and IRRs) noted above, there is an Internet Society[51] initiative that focuses on Mutually Agreed Norms for Routing Security (MANRS),[52] which aims to help reduce the most common routing system vulnerabilities. The objective of

MANRS is to improve the security and reliability of the global Internet routing system, based on collaboration among participants and shared responsibility for Internet infrastructure, setting a new norm for routing security and network operators. The specific categories of participants in MANRS include network operators and Internet exchange points, as well as content delivery networks and cloud providers. The MANRS program aims to raise awareness and create a culture of collective responsibility toward the security and resilience of the global routing system. It does this by providing a framework for network operators to better understand and address issues relating to the security and resilience of the routing system, to include best practices to prevent propagation of incorrect routing information, preventing traffic with spoofed source IP addresses, facilitating communication among operations, facilitating publication and validation of routing information on a global scale, and providing monitoring and debugging tools to participants. The MANRS initiative is continuing to gain traction and is certainly helping to make the routing system more secure.

Conclusion

While there are a broad array of other considerations related to attacks against the routing system, increased tooling and infrastructure to address the threat posed by route leaks and route hijacks will surely go a long way toward better securing the routing system. A stable and secure cryptographic number resource certification infrastructure is an absolute necessity to inform routing policies used to secure the routing system. However, the Internet community must be cautious to understand the implications of introducing potential new control points and systemic dependencies—and how they may impact the resilience, flexibility, and autonomy in operations for each participating network—that have made the current routing system so robust and successful.

Routing by rumor has served us well, and a decade ago it may have been ideal because it avoids systemic dependencies—but it is certainly past its prime in today's cyber environment. The accumulated improvements discussed here and elsewhere are changing rumors into knowledge and will ideally provide the foundation for a more secure Internet routing system in the future.

Currently, some of the discussion around the application of the public core definition within routing has focused on the importance of addressing routing hijacks. These remain difficult to address if intentional and launched by a sophisticated adversary in cooperation with one or more network operators.

Currently, some of the discussion around the application of the public core definition within routing has focused on the importance of addressing routing hijacks, such as those discussed above. These remain difficult to address if intentional and launched by a sophisticated adversary in cooperation with one or more network operators. However, one category of routing incidents has been a key focus thus far, and for this RPKI will help significantly. However, this solution also increases the operational importance of previously less relevant organizations (i.e., the RIRs) and the infrastructure they operate. This change and its ramifications must be fully understood and considered by all stakeholders (to include the memberships of the RIRs), given the full set of new obligations and resource allocation requirements that has been placed upon them. Together, however, such improvements represent a welcome maturation of the routing system away from just "routing by rumor" to "routing by fact."

Endnotes

1 Global Commission on the Stability of Cyberspace, Advancing Cyberstability, The Hague: The GCSC, November 2019. https://cyberstability.org/wp-content/uploads/2020/02/GCSC-Advancing-Cyberstability.pdf

2 "Norm on the Non-Interference with the Public Core," Global Commission on the Stability of Cyberspace, https://cyberstability.org/norms/#toggle-id-1

3 "Cyberstability Paper Series. New Conditions and Constellations in Cyber," Global Commission on the Stability of Cyberspace, https://cyberstability.org/paper-series/

4 Each of the five RIRs serve different regions. AFRINIC serves Africa and portions of the Indian Ocean, APNIC serves portions of Asia and portions of Oceania, ARIN serves Canada, many Caribbean and North Atlantic Islands, and the United States, LACNIC serves Latin America and portions of the Caribbean, and RIPE NCC serves Europe, the Middle East, and Central Asia.

5 "The Internet Engineering Task Force", https://ietf.org

6 "The CIDR Report", https://www.cidr-report.org/as2.0/

7 "The Interconnection Database", PeeringDB, https://www.peeringdb.com

8 "The CIDR Report", https://www.cidr-report.org

9 IEFT, "A Border Gateway Protocol 4 (BGP-4)," IETF Datatracker, RFC 4271, https://datatracker.ietf.org/doc/html/rfc4271

10 William Jr Haag, Doug Montgomery, William C. Baker and Allen Tan, Secure Inter-Domain Routing, (National Institute of Standards and Technology and National Cybersecurity Center of Excellence, 2016). https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/sidr-project-description-draft.pdf

11 K. Sriram, et al. "Problem Definition and Classification of BGP Route Leaks," Internet Engineering Task Force, RFC7908, (June 2016) https://www.rfc-editor.org/rfc/rfc7908.txt

12 Masahito Ando, Masayuki Okada, and Akira Kanaoka, "Simulation Study of BGP Origin Validation Effect against Mis-Origination with Internet Topology," 12th Asia Joint Conference on Information Security, (August 2017): doi 10.1109/AsiaJCIS.2017.17. https://www.researchgate.net/publication/319587923_Simulation_Study_of_BGP_Origin_Validation_Effect_against_Mis-Origination_with_Internet_Topology

13 Ryan Singel, "Pakistan's Accidental YouTube Re-Routing Exposes Trust Flaw in Net," Wired, February 25, 2008, https://www.wired.com/2008/02/pakistans-accid/

14 Ax Sharma, "Major BGP Leak Disrupts Thousands of Networks Globally," Bleeping Computer, April 17, 2021 https://www.bleepingcomputer.com/news/security/major-bgp-leak-disrupts-thousands-of-networks-globally/

15 "BGP Routing Leak Detection System", https://puck.nether.net/bgp/leakinfo.cgi

16 "Regional Internet Registries", The Number Resource Organization, https://www.nro.net/about/rirs/

17 "Internet Reouting Registry", http://www.irr.net

18 Danny McPherson, et al. "Considerations for Internet Routing Registries and Routing Policy Configuration", Internet Engineering Task Force, RFC 7682 (December 2015), https://tools.ietf.org/html/rfc7682

19 "List of Routing Registries", Internet Routing Registry, http://www.irr.net/docs/list.html

20 EXPLAIN RIRs

21 "Managing Route Objects in the IRR", RIPE Network Coordination Centre, https://www.ripe.net/manage-ips-and-asns/db/support/managing-route-objects-in-the-irr

22 "Contact Your Local Regional Internet Registry," The Number Resource Organization, https://www.nro.net

23 "NIST RPKI Monitor", National Institute of Standards and Technology, https://rpki-moni-

tor.antd.nist.gov

24 "Is BGP Safe Yet? No.", https://isbgpsafeyet.com

25 Ben Lutkevich, and Brien Posey, "What is a race condition?", TechTarget, last modified June 2021, https://searchstorage.techtarget.com/definition/race-condition

26 The President's National Security Telecommunications Advisory Committee, "NSTAC Report to the President on Communications Resiliency," CISA, May 2021, https://www.cisa.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20Communications%20Resiliency.pdf

27 "Regional Internet Registries are preparing to deploy "All Resources" RPKI Service," The Number Resource Organization, July 11, 2017, https://www.nro.net/regional-internet-registries-are-preparing-to-deploy-all-resources-rpki-service/

28 A. Newton et al., "RPKI Multiple "All Resources" Trust Anchor Applicability Statement," Internet Engineering Task Force, (July 2016), https://www.ietf.org/archive/id/draft-rir-rpki-allres-ta-app-statement-01.txt

29 Geoff Huston, "RPKI and Trust Anchors," APNIC, April 21, 2020, https://blog.apnic.net/2020/04/21/rpki-and-trust-anchors/

30 "IAB Statement on RPKI," Internet Architecture Board, April 3, 2018, https://www.iab.org/documents/correspondence-reports-documents/2018-2/iab-statement-on-the-rpki/

31 "IAB Statement on RPKI," Internet Architecture Board, January 27, 2010, https://www.iab.org/documents/correspondence-reports-documents/docs2010/iab-statement-on-the-rpki/

32 An illegitimate RPKI ROA could result in origin validation actions that suppress legitimate routing system announcements within ISP networks that are performing origin validation filtering. This issue exists whether or not a network's number resources were allocated from that specific RIR and even whether or not the network is currently using RPKI to publish ROAs. What specific route filtering actions a network operator might take based on the presence of a valid ROA that matches a route received from a BGP peer, or an invalid ROA, or no matching or "covering" ROA at all, is solely dependent on how RPKI-derived enforcement policies are currently implemented by each of the individual network operators in the routing system. These policy enforcement actions independently effectuated by each ISP may range from suppressing or completely filtering a route, to lowering or increasing the preference, or they may take no action at all.

33 Martin J. Levi, "RPKI—The required cryptographic upgrade to BGP routing," Cloudfare, September 19, 2018, https://blog.cloudflare.com/rpki/

34 Danny Cooper, et al. "On the Risk of Misbehaving RPKI Authorities," Boston University, Department of Computer Science, (November 2013) https://www.cs.bu.edu/fac/goldbe/papers/hotRPKI.pdf

35 "What is a Whois Service?," American Registry for Internet Numbers, https://www.arin.net/resources/registry/whois/

36 "ARIN's Trust Anchor Locator (TAL). Relying Party Agreement (RPA)," American Registry for Internet Numbers, https://www.arin.net/resources/manage/rpki/tal/

37 Felipe Victolla Silveira, "RIPE NCC and the Cloud: Draft Principles, Requirements and Strategy Framework," RIPE Labs, August 3, 2021, https://labs.ripe.net/author/felipe_victolla_silveira/ripe-ncc-and-the-cloud-draft-principles-requirements-and-strategy-framework/

38 "Notice of upcoming maintenance to ARIN's RPKI Infrastructure," American Registry for Internet Numbers, June 2, 2021, https://www.arin.net/announcements/20210602-rpki/

39 Where uptake has been slowest (for instance, across Africa), external support would be crucial, perhaps within currently envisioned state-led capacity-building (development assistance) programs being developed. Indeed, the crucial operations and needs of RIRs seem to have been somewhat ignored in the current debate on capacity building, and this example illustrates where additional resources could be meaningfully directed by the global policy community: RIPE, 47%

Valid; LACNIC, 37% Valid; APNIC, 34% Valid; ARIN, 20% Valid; AFRNIC, 13% Valid.

40 Louis Poinsignon, "The Internet is Getting Safer: Fall 2020 RPKI Update," Cloudfare, June 6, 2021, https://blog.cloudflare.com/rpki-2020-fall-update/

41 "Is BGP Safe Yet? No.", https://isbgpsafeyet.com

42 "The CIDR Report", https://www.cidr-report.org

43 Ryan Singel, "Pakistan's Accidental YouTube Re-Routing Exposes Trust Flaw in Net," Wired, February 25, 2008 https://www.wired.com/2008/02/pakistans-accid/

44 "BGP Case Studies," BGP.us, https://www.bgp.us/case-studies/

45 M. Lepinski, and K. Sriram, "BGPSEC Protocol Specification," Internet Engineering Task Force, RFC 8205, (September 2017) https://datatracker.ietf.org/doc/html/rfc8205

46 Danny McPherson et al. "Route -Leaks & MITM Attacks Against BGPSEC," Internet-Draft. IETF, (April 2014) https://datatracker.ietf.org/doc/html/draft-ietf-grow-simple-leak-attack-bgpsec-no-help

47 Catalin Cimpanu, "For two hours, a large chunk of European mobile traffic was routed through China," ZDNet, June 7, 2-19, https://www.zdnet.com/article/for-two-hours-a-large-chunk-of-european-mobile-traffic-was-rerouted-through-china/

48 Zak Doffman, "Russia and China 'Hijack' Your Internet Traffic: Here's What You Do," Forbes, April 18, 2020, https://www.forbes.com/sites/zakdoffman/2020/04/18/russia-and-china-behind-internet-hijack-risk-heres-how-to-check-youre-now-secure/?sh=7849a2a65b16

49 Andy Greenberg, "China Hijack 15% of Internet Traffic? More Like .015%," Forbes, November 19, 2010, https://www.forbes.com/sites/andygreenberg/2010/11/19/china-hijacks-15-of-internet-traffic-more-like-015/?sh=56eb0299223a

50 Dan Goodin, "Russian-controlled telecom hijacks financial services' Internet traffic," ArsTechnica, April 27, 2017, https://arstechnica.com/information-technology/2017/04/russian-controlled-telecom-hijacks-financial-services-internet-traffic/

51 "Internet Society," https://www.internetsociety.org

52 "MANRS," https://manrs.org/

About the Author

Danny McPherson is responsible for Verisign's information systems and services, as well as information and corporate security. He has actively participated in internet operations, research, and standardization since the early 1990s, to include serving on the Internet Architecture Board (IAB) and chairing an array of Internet Engineering Task Force (IETF) and other working groups and committees. He has authored several books, numerous internet protocol standards, network and security research papers, and other publications.

Previously, McPherson was CSO at Arbor Networks, where he developed solutions to detect and mitigate cyberattacks and performed pioneering research on Internet infrastructure evolution, as well as botnet and malware collection and analysis. Before that, he held technical leadership positions in architecture, engineering and operations with Amber Networks, Qwest Communications, Genuity, MCI Communications, and the U.S. Army Signal Corps.

Cyberstability Paper Series

New Conditions and Constellations in Cyber

Prioritizing Capacity Building as a Foundation for Cybersecurity and Stability

Christopher Painter
President, Global Forum on Cyber Expertise

Prioritizing Capacity Building as a Foundation for Cybersecurity and Stability

Christopher Painter | President of the Global Forum on Cyber Expertise

Capacity building is a foundational pillar in both building better technical cybersecurity for countries around the globe and achieving a more inclusive and coherent international set of international cyber policies. In addition, achieving better cybersecurity and combatting threats is a key enabler to achieving all the positive economic and social goals of our increasingly digitized world. In recognition of the important role it plays in achieving long-term cyberstability, the Global Commission on the Stability of Cyberspace ("GCSC") stated that cyber capacity building "is a prerequisite to adopting and implementing norms, ensuring accountability, taking other stability measures, and respecting human rights" and included a recommendation in its report that "[s]tate 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 needs of disparate parties,"[1]

However, despite the growing need, cyber capacity building remains underprioritized and underfunded—particularly when compared to other areas of traditional development, such as physical infrastructure, water, and health that are, themselves, increasingly dependent on digital systems and vulnerable to cyberattack. It is also given short shrift in development programs geared toward increasing connectivity or helping countries achieve a "digital transformation," even though those laudable goals could be undermined if digital networks are insecure. Moreover, though a growing number of countries and other stakeholders have engaged in cybersecurity capacity-building projects in recent years, those efforts have sometimes been uncoordinated with others—both ex-

Christopher Painter serves as the President of the Global Forum on Cyber Expertise—a global organization devoted to promoting and coordinating cybersecurity capacity building—and as a Commissioner on the Global Commission for the Stability of Cyberspace.

acerbating challenges posed by a relative lack of resources and limiting critical knowledge sharing among implementers, funders, and recipients that makes capacity-building efforts more effective. Fortunately, there has been a greater emphasis on cyber capacity building in high-profile recent United Nations processes devoted to cyber stability and ongoing significant global multi-stakeholder efforts to bolster and coordinate cyber capacity building. However, more focus, resources, and attention need to be paid to this vital area.

This paper discusses recent developments in capacity building in two United Nations processes: the Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security ("OEWG"), and The UN Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security ("GGE"). It then highlights the work of the Global Forum on Cyber Expertise ("GFCE")—a multistakeholder organization dedicated to promoting cyber capacity building prioritization, knowledge sharing, and better coordination among donors, implementers and recipients—that is ideally positioned to take forward many of the UN reports' recommendations.

It then explores a number of challenges to effective cyber capacity building, including the failure of many states to recognize cybersecurity as a core national and economic security priority, the lack of integration between the cybersecurity capacity building and traditional development communities, and the need for greater participation in and political awareness of the GFCE as a global coordinating community. Finally, a number of recommendations are made to address these challenges and strengthen cyber capacity building in the future.

The need for governments, the private sector, and other entities to prioritize cybersecurity has been amply illustrated over the last year by frequent and significant malicious cyber incidents that have ranged from nation state-sponsored intelligence gathering campaigns to criminally sponsored ransomware attacks that have targeted health care providers and impacted critical infrastructure and vital services to the public, such as food supplies and fuel. The case for better cybersecurity has been further strengthened by the pandemic, which has highlighted the increasing dependence of both developed and developing countries on information and communication technologies, and the vulnerability of those systems to interference by malicious actors. During the same period, the need for policy and diplomatic expertise on cyber issues become ever more apparent as these issues continue to be debated at a high level in the United Nations, regional bodies, and bi-laterally between countries. Yet, despite the increased attention being paid to cybersecurity and cyber policy issues, many countries lack the technical, institutional and policy capability to respond to malicious cyber events, including the capability to cooperate internationally, and many lack the ability or expertise to fully participate in the many international debates that are shaping the future of cyberspace.

Despite the increased attention being paid to cybersecurity and cyber policy issues, many countries lack the technical, institutional and policy capability to respond to malicious cyber events, including the capability to cooperate internationally.

A country's ability to realize the economic and social benefits that information and communication technologies bring is dependent on its ability to deal with a rising tide of threats to those systems. Further, it is almost axiomatic that the cybersecurity of any country in the world is dependent on the security of others, given that malicious actors will take advantage of any "weakest link" to route their attacks and intrusions. Accordingly, both domestic and global security and prosperity suffer when countries are not equipped to handle cyber threats. It is equally true that participation and understanding by as many countries as possible will help implement international law, norms of

appropriate state behavior, and confidence-building measures and lead to a greater and more sustainable framework for cyber stability.

A substantial answer to both preparing countries to deal with cyber threats and ensuring they can more fully participate in policy implementation is cyber capacity building. Cyber capacity building, or, more particularly, cybersecurity capacity building, is a broad term describing structured assistance programs around cybersecurity for developing countries. It encompasses technical training, structural or institution building, and other policy-oriented programs. Technical training includes programs directed at training law enforcement officers how to investigate cybercrime and training technical first responders. Structural and institutional capacity building includes helping countries develop national-level Computer Security Incident Response Teams ("CSIRTs") and develop national-level coordination mechanisms. Policy capacity building includes helping countries to develop national cybersecurity strategies, to develop cybercrime and other legislation, to train diplomats on cyber issues and to work with diplomats and other senior policy makers to help implement the voluntary norms of behavior and cyber confidence-building measures ("CBMs") agreed to in the UN or other international forums. These different forms of capacity building often overlap but all are important for a country to achieve greater cyber capabilities, maturity, and the ability to meaningfully cooperate with international partners. Not surprisingly, the pressing need for greater cyber capacity building received increased and welcome attention in two key UN processes over the last couple of years: the OEWG and the GGE.

During the organizational and negotiating sessions of the recently concluded OEWG, involving all 195 UN member states, numerous countries raised the need for cyber capacity building. Although the OEWG dealt with a wide range of sometimes esoteric cyber stability issues—including norms of acceptable state behavior, CBMs, the application of international law and existing and potential threats—many less developed countries made the case that they urgently needed concrete technical and policy assistance. In response to this, several lengthy formal OEWG sessions were devoted to capacity building. Capacity building was also highlighted as a topic in the informal multistakeholder OEWG session.

A significant portion of the OEWG final consensus report was devoted to capacity building. The OEWG found that capacity building is inextricably linked to cyber stability, stating that capacity building "is of particular relevance to developing States, in order to facilitate their genuine participation in discussions on ICTs in the context of international security and their ability to address vulnerabilities in their critical infrastructure. It plays an important enabling function for promoting adherence to international law and the implementation of norms of responsible State behaviour, as well as supporting the implementation of CBMs."[2]

The OEWG also agreed to a set of "capacity building principles" by which to guide global efforts.[3] These principles focused on three broad areas: Process and Purpose, Partnership, and People. Among other things, the principles state that capacity building should be sustainable, results oriented, evidence based, politically neutral, transparent, and with a shared objective of "an open, secure, stable, accessible and peaceful ICT environment."[4] They also urge that capacity building "should be based on mutual trust, demand-driven, correspond to nationally identified needs and priorities, and be undertaken in full recognition of national ownership" and that it "should respect human rights and fundamental freedoms, be gender sensitive and inclusive, universal and non-discriminatory."[5]

Among other things, the OEWG report notes several types of concrete capacity building activities, including: the development of national cybersecurity strategies, building CSIRTs, and establishing

platforms for best practices and information sharing.[6] And, the OEWG report notes the importance of policy capacity building—including diplomatic capacity—in addition to technical and structural efforts: "[i]n addition to technical skills, institution-building and cooperative mechanisms, States concluded that there is a pressing need for building expertise across a range of diplomatic, legal, policy, legislative and regulatory areas. In this context, the importance of developing diplomatic capacities to engage in international and intergovernmental processes was highlighted."[7]

Helpfully, in its recommendations, the OEWG report recognizes that current resources are limited for capacity building and encourages "states and other actors ... to offer financial, in kind, or technical assistance" if they are in a position to do so.[8] It also recommends that "promotion of coordination and resourcing of capacity-building efforts, including between relevant organizations and the United Nations, should be further facilitated."[9] And, the OEWG recommends that "States continue to consider capacity-building at the multilateral level, including exchange of views, information and good practice."[10] Unfortunately, it only makes a somewhat muted reference to the role of non-governmental stakeholders, stating that "the valuable contributions of other relevant stakeholders to capacity building activities" were recognized.[11]

The UN GGE, comprised of a selection of twenty-five countries, that largely ran parallel to the OEWG and issued its report following the OEWG report, also devoted substantial attention to capacity building. Like the OEWG, the GGE consensus report noted the foundational role of capacity building, stating that it "underscores the importance of cooperation and assistance in the area of ICT security and capacity-building and their importance to all elements of the Group's mandate."[12] The report also ties capacity building to a state's ability to both detect and respond to threats and, importantly, "ensures that all States have the capacity to act responsibly in their use of ICTs."[13] The GGE report further notes certain areas of capacity building that are central to the voluntary norms that it discusses and further articulates earlier in the document, including protection of critical infrastructure (norm 13(g)), and having the ability to request and respond to calls for assistance when malicious ICT activity affects or emanates from their territory (norm 13(h)). The GGE report further recommended that capacity building be further strengthened in a number of areas, including technical, structural, and policy assistance. These areas include those called out in the OEWG report and which improve the security of critical infrastructure; building the technical, legal, and policy capabilities to detect, investigate and resolve ICT incidents; deepening understanding of how international law applies to cyberspace; and implementing agreed-upon voluntary norms of responsible behavior.[14]

The GGE report gives a more full-throated endorsement of multistakeholder involvement in capacity building than does the OEWG report, stating that "[i]ncreased cooperation alongside more effective assistance and capacity-building in the area of ICT security involving other stakeholders such as the private sector, academia, civil society and the technical community can help States apply the framework for the responsible behaviour of States in their use of ICTs."[15] The report also notes that such efforts are "critical to bridging existing divides within and between States on policy, legal and technical issues relevant to ICT security."[16] In addition, the report recommends that "States should consider approaching cooperation in ICT security and capacity-building in a manner that is multi-disciplinary, multi-stakeholder, modular and measurable."[17] The report also recognizes that this effort will require broad collaboration and coordination, including "working with the United Nations and other global, regional and sub-regional bodies and alongside other relevant stakeholders to facilitate the effective coordination and implementation of capacity-building programmes, and by encouraging transparency and information sharing on their effectiveness."[18]

Like the OEWG report, the GGE report recognizes the need for greater capacity-building resources, stating that "[i]n order to bridge digital divides and ensure all States benefit from these and oth

er areas of assistance and capacity-building, States are encouraged to commit, where possible, financial resources as well as technical and policy expertise, and to support countries requesting assistance in their efforts to enhance ICT security."[19] However, though the report states that capacity building "may contribute to meeting other objectives of the international community, such as SDGs (Sustainable Development Goals),"[20] it stops short of stating that cyber capacity building can be instrumental in achieving the SDGs, as some had urged in the OEWG.

The strong language of the two UN reports creates an opportunity to promote practical cyber capacity building as a priority issue and to strengthen and gain greater recognition for existing capacity-building efforts.

While the increased attention to capacity building in both the OEWG and GGE reports is welcome, as are the exhortations in both reports for countries and other stakeholders to work together and better resource this endeavor, it remains to be seen what actual impact these reports will have in practical terms. Given the interest level especially among developing countries, it is likely that capacity building will again be a topic on the agenda of the new five-year OEWG that is just beginning its work. However, it is unclear what further progress can be made in that long-term government-focused forum when capacity building is an urgent current priority involving many stakeholders. There is also the proposal for a Program of Action by a number of states that contemplates greater nonstate stakeholder involvement and expressly mentions capacity building as one goal.[21] However, the fate, direction, and timing of that proposal remains unclear. Nevertheless, regardless of further UN institutional activity, the strong language of the two UN reports creates an opportunity to promote practical cyber capacity building as a priority issue and to strengthen and gain greater recognition for existing capacity-building efforts. Indeed, an existing multistakeholder cyber capacity-building coordination platform, The Global Forum on Cyber Expertise, can play a key role in continuing to implement many of the precepts from the UN reports.

The GFCE is a multistakeholder organization of over one hundred and forty-five members and partners, including over sixty governments, numerous private sector, civil society, and academic institutions and a number of regional and international organizations. It was established in 2011 in recognition of the need to promote cyber capacity building and to avoid unnecessary duplication of and conflict between capacity-building programs.[22] Its mission is to "strengthen cyber capacity and expertise globally through international collaboration and cooperation."[23] It accomplishes this by "connecting needs, resources, and expertise and by making practical knowledge available to the global community." In order to avoid duplication and to make sure that gaps are adequately addressed, the GFCE coordinates regional and global cyber capacity projects, shares knowledge and expertise, and matches individual needs to offers of support from the GFCE community. It provides these services through a global capacity-building portal, the Cybil Portal, populated by publications, tools, best practices, and other material; a recently launched global capacity building research agenda that seeks to identify and fill gaps in capacity building knowledge; and a clearing house mechanism that connects countries needing help in a particular area with a tailored suite of funders and implementers who can fill that need.

The GFCE is organized substantively around five substantive working groups: Cyber Security Strategy and Policy (including a Task Force on norm implementation, CBMs, and diplomacy); Cyber Incident Management and Critical Infrastructure Protection, Cybercrime; Cyber Security Culture and Skills; and Cybersecurity Standards. The Working Groups meet regularly to identify needs, assist with coordination of projects, and provide a platform for sharing by the community. In

addition, the GFCE is a platform for high-level discussion, organizing biannual meetings to assess progress and hold policy discussions on ways and means of responding to emerging challenges in the cyber capacity-building domain. The GFCE is intended to be global but also work with regional efforts, convening a number of regional meetings in the last year. In addition, it works with regional organizations including the Organization of American States and recently launched a major initiative with the African Union. It is not intended to replace the capacity building efforts and programs of its many members and partners, but, instead, is intended to strengthen and highlight them and make sure others can benefit from lessons learned.

The substantive areas of focus for the GFCE easily map to the areas of focus called out by the OEWG and GGE. Moreover, several participants in the OEWG expressed a desire for greater coordination of capacity building efforts and expressed some confusion of where they could go if they needed capacity building assistance. The GFCE was established to provide that greater coordination and can provide an entry point for a country in need to a community that is focuses on these issues. Given the current dire need for cyber capacity building, it makes sense, as the GCSC recommended, to leverage existing organizations, such as the GFCE, to help meet that demand.[24]

While the GFCE brings greater coordination and focus to cyber capacity building and the OEWG and GGE reports bring greater attention, a number of significant challenges remain. Despite the growing number of cyber capacity-building projects, the field is still chronically under-resourced and under prioritized. In part, this is due to cybersecurity as a field still struggling to be integrated as a true national and economic security issue for countries. Fortunately, this is finally changing as a number of countries are now recognizing the importance of cybersecurity, both because of the increased reliance on digital technologies during the pandemic and the increase of disruptive ransomware and other malicious cyber incidents. Nevertheless, more progress needs to be made in elevating both cybersecurity and cybersecurity capacity building as core priority issues, particularly at senior government policy levels.

Despite the growing number of cyber capacity-building projects, the field is still chronically under-resourced and under prioritized. In part, this is due to cybersecurity as a field still struggling to be integrated as a true national and economic security issue for countries.

In part, the relative lack of attention and resources for cybersecurity capacity building is attributable to its lack of integration with larger development programs or digital strategies. For example, the UN Sustainable Development Goals have attracted both political attention and substantial resources. While cybersecurity is a key enabler of many of those goals, there is no formal clear acknowledgement of that relationship. Similarly, many countries' traditional development programs treat cyber as a law enforcement or military issue that is outside their normal mandate. While this is changing—the US, UK, and EU traditional development agencies, among others, are moving into cyber capacity-building projects—the general approach of the traditional development community should be expanded.

Though the GFCE has been successful as a coordination platform and its membership has grown significantly in its six-year existence, many countries and other entities are not yet members or partners and many potential partners are unaware of the coordination and information sharing services it offers. This limits its effectiveness as a much-needed coordination platform and exacerbates resource shortfalls. Even among existing GFCE members, information sharing on programs and experience could be better. Moreover, the GFCE has built a cyber capacity community at the expert level but would benefit from a more sustained connection to high-level policy makers. The

GFCE was launched at the Global Conference on Cyber Space (a.k.a., "The London Process") in the Hague in 2015. The GCCS brought together ministers, CEOs, and other high-level stakeholders and provided a good platform from which to link expert-level work to senior political priorities. Unfortunately, the GCCS has been moribund since 2017 and there is no high-level multistakeholder forum devoted to cyber capacity building. Finally, the GFCE Secretariat structure is relatively small given the breadth and likely growth of its mission.

Although not exhaustive, the following recommendations are proposed to strengthen cyber capacity building and the cyber capacity-building coordination ecosystem:

Promote Cyber Capacity Building as a Global Priority

Keep cyber capacity building as a key agenda item in new UN processes and in other international venues. Given the foundational nature of cyber capacity building and its importance, particularly to the developing world, it should remain a key topic in the new cyber Open-Ended Working Group and the Program of Action. It should also be an area of focus in multistakeholder processes such as the Paris Call.

Convene a high-level, multistakeholder cyber capacity building focused summit. With the apparent demise of the Global Conference on Cyberspace, there is no high-level, multistakeholder forum devoted to cybersecurity issues, and no such forum devoted to cyber capacity building. A forum that attracts high-level government officials, including foreign ministers, senior private sector representatives, and other senior civil society and academic participants not only would lead to a higher profile of the issue as a mainstream priority, but also help attract greater resource commitments and, potentially, validate a global cyber capacity building agenda. Moreover, a meeting that brings the cyber community and the traditional development community together could break down existing silos and substantially enhance cyber capacity building resources and effectiveness. The GFCE together with a number of partners, including the World Bank, the World Economic Forum, and the Cyber Peace Institute, is currently planning to hold such a meeting in 2022 in Washington, DC.

Increase Resources and Link Cyber Capacity Building to Development

Clearly state that cyber capacity building is foundational to the UN Sustainable Development Goals. Although the UN GGE Report referenced the UN SDGs, it stopped short of stating that cyber capacity building will be a key enabler of achieving those goals. Part of the reticence to make such a statement was that the GGE was a process under the First Committee and that the SDGs were not part of the jurisdictional mandate of that group. Bringing the traditional development community and cyber capacity building community together[25] will benefit both groups, so interaction and a higher-level statement to this effect—perhaps at the Secretary General level—will help these two communities work together.

Use existing efforts of traditional development agencies in cyber capacity building as a model for other potential funders. As USAID, the UK's DFID, and the World Bank, among others, step up cyber capacity-building programs, these efforts should be used to persuade the rest of the traditional development community to fund and engage in these programs. For example, USAID recently published a "Cybersecurity Primer: How to Build Cybersecurity into USAID Programming" that details how cybersecurity is important to its development portfolio and how to em-

bed cybersecurity into its programming cycle. The Primer is meant for both USAID staff and as "a resource on cybersecurity for the broader development community and spotlights how USAID's approach to cybersecurity in development is evolving. "

Expand the definition of what qualifies as development assistance to include cyber capacity building. Much of the traditional development community looks to the Organization for Economic Cooperation and Development's Development Assistance Committee (OECD DAC) for guidance on traditional development projects. However, its criteria for Official Development Assistance (ODA) projects excludes the promotion of donors' security interests, which may be read by some to exclude or at least limit projects geared to cybersecurity capacity building. This could be remedied if the OECD DAC would make clear that the ODA includes cybersecurity projects, or amend it to make that clear, and aid in their creation and promotion.

Translate the UN OEWG and GGE statements that countries should further support and resource cyber capacity building into action. Many states are currently investing in cyber capacity building on a project basis, and those efforts can be built upon and used to catalyze other donors and implementers. For example, the U.S., U.K., Estonia, and the Netherlands, among others, all have significant individual capacity building efforts that range from technical training to CSIRT building to the application of international law to cyberspace. If several active states collectively announce significant capacity-building projects and funding, and work with other countries to do the same, the pool of resources will be increased as will the profile of those efforts. Several countries have already taken the step of working with the World Bank to fund a cybersecurity development fund, but that initiative could also be expanded and given more visibility. Further, despite cyber capacity building being a true multistakeholder endeavor, only a few private sector entities and philanthropic foundations fund capacity-building efforts.[26] Getting more private sector entities around the globe—both tech and non-tech entities, such as those involved in financial services—into the capacity-building field is important but requires a stronger narrative of why it is in their interest. Similarly, a concerted campaign is needed to broaden support from the philanthropic community.[27]

Foster and Strengthen Mechanisms for Better Coordination

Expand and resource the GFCE. The GFCE is a relatively mature, multistakeholder community that is ideally positioned to coordinate and help implement the capacity-building recommendations from the OEWG and GGE. For it to meet this expectation and deal with the increased demand for cyber capacity building, it will need greater institutional support and resources. Moreover, the GFCE must continue to grow and add more countries, intergovernmental organizations, private sector, civil society, and academic organizations to its already impressive list of members and partners. Finally, though many in the cyber capacity-building field are aware of the GFCE, it needs to achieve a higher profile so that countries are aware of the resources and services it offers, and those involved in capacity building can use its platform to share their expertise. The planned upcoming high-level capacity building conference is designed, in part to achieve that higher profile. By strengthening the GFCE as an existing mature platform rather than creating new coordination organizations, scarce resources are maximized and duplication and confusion averted.

Encourage greater information sharing of cyber capacity building projects and activities. Though many states and other parties share some information on their projects and activities, there is some reluctance by funders and implementers to share the details of their current efforts. A lack of sharing, for example on the Cybil Portal, deprives other players and regions from

benefiting from lessons learned, it hampers coordination, leads to potential duplication, and limits helpful input that the sharing party might otherwise receive. Of course, states and other stakeholders have some legitimate concerns about confidentiality and proprietary information, still, for the benefit of the entire cyber capacity building community, greater sharing and transparency should be encouraged and be the default.

Leverage and connect regional capacity building efforts. As important as global efforts are, much great capacity building work is done at the regional level in response to unique regional demands and expertise. The Organization for American States, ASEAN, the African Union, and the European Union all are engaged in strong regional efforts. The GFCE provides a a forum for bringing these efforts together. It is developing a regional focus, partnering with all of the aforementioned regional bodies, and spearheading a regional effort in the Pacific Islands. Sharing lessons learned, programs, and expertise among these regional efforts will serve to strengthen all of them.

The focus on cyber capacity building in the recent UN OEWG and GGE reports, coupled with the recent global political focus on cybersecurity as a national and economic security imperative, creates a unique and possibly fleeting opportunity to substantially elevate cyber capacity building as a priority and enable a sustained international effort. The GFCE is well positioned to help take this forward, and can work with other institutions, countries, and stakeholders to make effective, coordinated cyber capacity building a reality. If we fail to seize this opportunity, including by failing to address the challenges described in this paper, we will not only fail to meet the needs and expectations of developing countries, but will put at risk all of world's ability to combat growing cyber threats or to achieve long term cyberstability. That is a price that no country, business or responsible stakeholder can afford.

If we fail to seize this opportunity, including by failing to address the challenges described in this paper, we will not only fail to meet the needs and expectations of developing countries, but will put at risk all of world's ability to combat growing cyber threats or to achieve long term cyberstability.

Endnotes

1 Global Commission on the Stability of Cyberspace, "Advancing Cyberstability. Final Report," The GCSC, November 2019, page 26, recommendation 3. https://cyberstability.org/report/

2 United Nations General Assembly, "Open-ended working group on developments in the field of information and telecommunications in the context of international security. Final Substantive Report," A/AC.290/2021/CRP.2, United Nations, March 10, 2021, page 8, para. 54. https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

3 The OEWG Capacity Building Principles are partly modeled on those adopted by the Global Forum on Cyber Expertise (that were, in turn, modeled after Bussan Partnership for Effective Development Cooperation). GFCE, "Global Agenda for Cyber Capacity Building. Putting Principles into Practice," The GFCE, November 21, 2017, https://thegfce.org/wp-content/uploads/2020/06/GACCBversion_21nov.pdf. The OEWG principles differ from the GFCE ones in highlighting sovereignty and confidentiality.

4 United Nations General Assembly, "Open-ended working group on developments in the field of information and telecommunications in the context of international security. Final Substantive Report," A/AC.290/2021/CRP.2, United Nations, March 10, 2021, page 8, para. 56. https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

5 Ibid.

6 Ibid. para. 61.

7 Ibid. para. 60.

8 Ibid. para. 66.

9 Ibid.

10 Ibid.

11 Ibid.

12 Group of Governmental Experts, "Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security," A/76/135, July 14, 2021, Para. 87. https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf

13 Ibid. para 88.

14 Ibid. para 89.

15 Ibid. para 87.

16 Ibid.

17 Ibid. para 92.

18 Ibid.

19 Ibid. para 90.

20 Ibid.

21 France et al., "The future of discussions on ICTs and cyberspace at the UN," United Nations, August 10, 2020, https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-future-of-cyber-discussions-at-un-10-08-2020.pdf The framing paper notes that one goal is to "[s]tep up cooperation and capacity building, building on the implementation meetings, by defining what the most urgent needs are and by fostering coordination between States when relevant. We believe that capacity building will be crucial to ensure the success of a PoA."

22 The Government of the Netherlands, joined by a number of other governments, private sector and civil society organizations, founded the GFCE at the GCCS in 2011. The GFCE was launched as an independent foundation in February 2020 alongside the second meeting of the OEWG.

23 "About the GFCE," The GFCE, https://thegfce.org/about-the-gfce/

24 See Global Commission on the Stability of Cyberspace, "Advancing Cyberstability. Final Report," The GCSC, November 2019, page 26, recommendation 3: "all parties should leverage existing organizations, including the multistakeholder Global Forum on Cyber Expertise, that are focused on capacity building ..." https://cyberstability.org/report/

25 For a thorough discussion of bridging the gap between the digital component of the traditional development and cybersecurity capacity building communities, see Melissa Hathaway and Francesca Spidalieri, "Integrating Cyber Capacity into the Digital Development Agenda," Global Forum on Cyber Expertise (GFCE) Foundation, November 2021.

26 For example, the Gates Foundation and Microsoft are funding different aspects of the GFCE's work in Africa.

27 Though garnering greater philanthropic support of cyber has been a goal of the great work of the Hewlett Foundation, those efforts have had only modest success to date. In April 2021, over thirty organizations and individuals signed a letter urging greater philanthropic giving to cybersecurity programs. Tim Starks, "A push for cybersecurity philanthropic giving launches," CyberScoop, April 16, 2021, https://www.cyberscoop.com/philanthropic-giving-cybersecurity-open-letter-craig-newmark/. Among other things, the letter asserts that cybersecurity grants were only a tiny fraction of peace and security program grants and urges greater giving, particularly by the tech sector.

About the Author

Chris Painter is a globally recognized leader and expert on cybersecurity and cyber policy, Cyber Diplomacy and combatting cybercrime. He has been on the vanguard of U.S. and international cyber issues for over thirty yeas. While in government he served first as a federal prosecutor of some of the most high-profile cybercrime cases in the U.S. and then as a senior official at the Department of Justice, Senior Director of Cyber Policy at the National Security Council, and finally as the top cyber diplomat at the State Department. In this last role, Mr. Painter established the first high-level office dedicated to cyber diplomacy at a foreign ministry in the world. Mr. Painter currently serves as the President of the Global Forum on Cyber Expertise Foundation, a multistakeholder organization devoted to promoting and coordinating cyber capacity building. He also serves on the Board of the Center for Internet Security, is a non-resident Senior Advisor at the Center for Strategic and International Studies, an Associate Fellow at Chatham House, and is on the Public Sector Advisory Board for Palo Alto Networks. He was also a co-chair of the Ransomware Task Force and a Commissioner on the Global Commission on the Stability of Cyberspace.

Cyberstability Paper Series

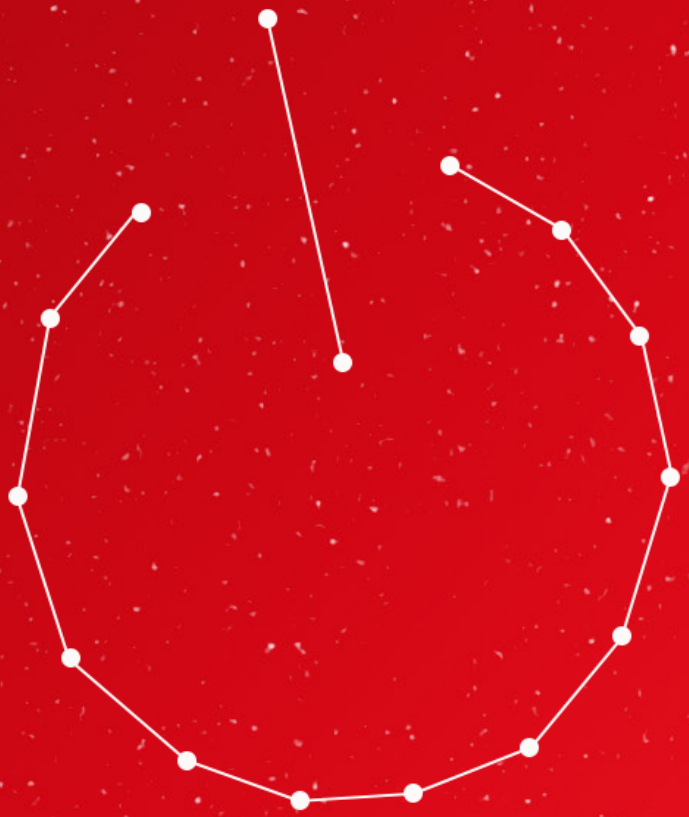
New Conditions and Constellations in Cyber

Disconnecting from Cyberstability

An Assessment of how Internet Shutdowns in the Democratic Republic of Congo, Tanzania, and Uganda Undermine Cyberstability

Moses Owiny
Founder and CEO of the Centre for Multilateral Affairs (CfMA)

Sheetal Kumar
Senior Programme Lead at Global Partners Digital



Disconnecting from Cyberstability: An Assessment of how Internet Shutdowns in the Democratic Republic of Congo, Tanzania, and Uganda Undermine Cyberstability

Moses Owiny | Founder and CEO of the Centre for Multilateral Affairs (CfMA)

Sheetal Kumar | Senior Programme Lead at Global Partners Digital

The aim of this article is to assess how Internet shutdowns undermine cyberstability as defined by the Global Commission on the Stability of Cyberspace (GCSC). According to the GCSC framework, cyberstability means that 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.[1] The assessment of how shutdowns undermine cyberstability is based on Internet shutdowns in three neighboring countries—the Democratic Republic of Congo (DR Congo), Tanzania, and Uganda—over the past five years, and is conducted according to the GCSC's four cyberstability principles: a) Responsibility, b) Restraint, c) Requirement to act, and d) Respect for human rights. We review select cases of shutdowns in each country, describing their main characteristics (e.g., the services affected, duration of the shutdown, and the measured impact). The selection of countries was based on the

Moses Owiny is the Founder and CEO at the Centre for Multilateral Affairs (CfMA) in Uganda. In June 2021, he served as an external co-chair and Programme Committee member for the 10th edition of RightsCon under the category "Cyber Norms, Accountability, and Practice."

Sheetal Kumar is Senior Programme Lead at Global Partners Digital. Her recent work has focused on applying human-centric approaches to cyber policy, including cyber norms.

frequency of shutdowns in the East and Central Africa region and opportunities to build on existing literature, which has yet to assess the issue of shutdowns according to the concept of cyberstability. Our conclusion is that every cyberstability principle is impacted by Internet shutdowns and that States and telecommunications companies have obligations and responsibilities to end the practice of shutdowns. Civil society, the technical community, and academia also have a role to play in keeping States and telecommunications companies accountable for the negative impact caused by shutdowns.

Through this assessment, we illustrate how and where shutdowns harm cyberstability, expose the gaps required to further understand the relationship between shutdowns and cyberstability, and highlight existing relevant recommendations that would support countries' regulatory frameworks to uphold, rather than undermine, cyberstability. Of particular note is the work the UN Human Rights Council has done to highlight the impact of Internet shutdowns on human rights. In 2021, the UN Special Rapporteur on Freedom of Association and Assembly issued a highly comprehensive report focused on Internet shutdowns, complete with recommendations for States, investors, telecommunications companies, and the UN institutions. We have reviewed these recommendations and, in line with the cyberstability framework, select the most relevant to the cyberstability framework.

We employ the following definition of Internet shutdowns, which are also referred to as network disruptions or "kill switches": "an intentional disruption of Internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information." This definition has been developed by experts and widely employed, including by the NGO Access Now's "Keep It On" campaign.[2] The definition covers the range of shutdowns explored in the country case studies, for instance, those affecting social media and Short Message Services (SMS) (Tanzania), a total outage of Internet services followed by partial restoration (Uganda), and blocking of social media and SMS (DR Congo). Notably, the definition does not cover other forms of information control, such as censorship or stringent content moderation.[3] However, as is highlighted in the country case studies, shutdowns are often utilized to exert information control as part of broader authoritarian trends, which can include harassment of journalists, regulatory frameworks that stifle free expression, suppression of political opponents during an election, and other measures.

Shutdowns are often utilized to exert information control as part of broader authoritarian trends.

Beginning with the DR Congo, we first provide an overview of each country's Internet landscape, including information about the shutdowns experienced in each country. We then assess how each cyberstability principle was affected by the shutdowns.

The DR Congo has an estimated population of over 70 million people, and among the lowest technology penetration rates in the region: 17% Internet penetration and 39.7% mobile phone penetration[4] as of 2019. As in Uganda, the Internet disruption trend in DR Congo first began in 2011 when SMS were blocked for 25 days in December of that year.[5] The second shutdown occurred in January 2015 when both SMS and Internet services were blocked as citizens protested against the proposed electoral bill; the disruption lasted four days. The third shutdown occurred on December 19, 2016 when social media was blocked a day after former president Joseph Kabila was expected to step down as Head of State. The fourth shutdown occurred in December 2018 during the Presidential election and resulted in the Internet and SMS being blocked for 20 days.[6]

As of 2019, the DR Congo had four mobile operators: Vodacom RDC, Airtel Congo, Orange RDC, and Africell RDC, with Vodacom as the leader in the voice segment with 35.2% of the market, followed be Orange at 30%, Airtel at 23.9%, and Africell at 10.9%.[7] The DR Congo has experienced many Internet shutdowns over the years as noted above, and this ranges from complete country-wide shutdowns to targeted regional shutdowns of social media platforms. The laws that govern telecom companies in the DR Congo contain sections that specifically mandate that license holders may be ordered to shut off access to their networks due to concerns of national security and public order.[8] For example, all three international telecom companies in the country—Vodacom (Vodafone controlled company), Millicom, and Bharti Airtel—all publicly acknowledged receipt of an order to suspend Internet service.[9]

Internet shutdowns prevent access to information and impedes freedom of expression, assembly, association, and opinion. It impedes rights to livelihood and work, education and health.[10] For example, the Framework for Calculating the Economic Impact of Internet Disruptions in Sub-Saharan Africa report notes that the DR Congo loses at least 1,936,911 United States Dollars (USD) per day during an Internet disruption[11]. Shutdowns impact the ability of journalists to receive information that is newsworthy but also curtail their ability to share essential information with society. This violates the rights to a free press and restricts both the right to access information as well as the right to freedom of expression.[12]

Internet shutdowns prevent access to information and impedes freedom of expression, assembly, association, and opinion. It impedes rights to livelihood and work, education and health.

Tanzania has an estimated population of 61 million and an Internet penetration rate of 49%.[13] In October 2020, ahead of the general elections in Tanzania, the government ordered the blocking of widely used messaging and social media applications, including WhatsApp, Twitter, Instagram, Facebook, and Google services[14] as well as local social media including the widely popular Jamii Forum. This followed a directive by the Tanzania Communication Regulatory Authority which ordered telecom companies to suspend "bulk SMS messaging" and voice communications as well as individual text messages with certain "keywords," making it effectively impossible for millions of Tanzanians to communicate during this time.[15] While this was not a wholesale blocking, it effectively resulted in people not being able to send text messages and not being able to communicate via the most commonly used messaging platforms over the Internet. The government's justification for the shutdown was "national security and concern for the fairness of the electoral process."[16] In addition to the blocking of social media and text, it was reported that media websites, including websites reporting on election fraud or election events, were blocked and attempts by the government to slow down Internet connections were also documented[17] Virtual Private Networks (VPNs) were banned, although they continued to be accessed during this shutdown.

These attempts to control information and dissent play out in a wider context/trend of shrinking democratic space in the country, including censorship and restriction of the work of journalists, drastically affecting the ability of Tanzanians to exercise their right to freedom of expression. For example, as was covered and commented on widely at the time by both the media and human rights activists, the election shutdown was part of a wider set of information control tactics, including legislation clamping down on foreign press by outlawing international press from covering developments in the country without local media partnerships.[18] It also included other legislation requiring bloggers to register and pay license fees.[19]

In terms of the impact of the shutdown in 2020, analysts said it was "immense," leaving "millions without effective communication tools" across Tanzania and ahead of the general elections.[20] Tanzania has millions of Internet users, and many of these, especially young people, were unable to earn money without the Internet.[21] Case studies of victims collected by Access Now illustrate some of the harm caused, including an inability to work, to complete educational training, and to run businesses and make sales.[22]

Uganda is a landlocked country with an estimated population of 41.6 million people[23] and 20.1 million Internet subscribers,[24] as of April 2020. President Yoweri Museveni won re-election in the January 2021 polls with 59%, despite widespread irregularities, extending his rule to 40 years in power[25] In the lead up to the elections from January 11 to 13, 2021, social media access was blocked and the downloading of some VPNs restricted. This was followed by an Internet blackout, which was lifted by January 18, 2021.

Internet shutdowns in Uganda form part of a more long-standing trend in the country to disrupt communications and the free flow of information among citizens prior to and during elections. In the 2006 elections season, the government instructed Internet Service Providers (ISPs) to block access to the website of Radio Katwe for allegedly publishing "malicious and false information" against the ruling National Resistance Movement (NRM) party and its presidential candidate. At the time, this incident received little public outcry. Yet, it set a troubling new standard in the country. In 2011, the government again instructed ISPs to block access to Facebook and Twitter for 24 hours, during opposition protests dubbed "walk to work" over rising fuel and food prices. However, following this directive, some Internet Service Providers (ISPs) did not respond, claiming they received the directive after the dates specified in the directive. On the eve of the presidential election on February 18, 2016, authorities cut off access to Twitter, Facebook, WhatsApp, YouTube, and Mobile Money services.[26] Later that year, after a disputed election that saw the swearing in of President Museveni in May, social media platforms, including Facebook, WhatsApp, and Twitter, were blocked (with the exception of Mobile Money).[27] More recently, beginning in 2018 and upon the introduction of taxes to access social media platforms, authorities have threatened to block VPNs for those using them to bypass paying the taxes.[28]

The very nature of the shutdowns displayed the multiple actors required to exert control over access to the Internet.

Justifications for the various shutdowns in Uganda by the state have included threats to "national security" from public unrest, the elimination of "the connection and sharing of information that incites the public"[29] and protection of the "national interest".[30]

In the following section, we consider how each of the principles of the cyberstability framework is impacted by the shutdowns discussed above. We take each principle in turn, beginning with the "Responsibility" principle.

The GCSC's framework "responsibility principle" states that everyone is responsible for ensuring the stability of cyberspace. This includes individuals, groups such as civil society, the private sector, technical communities, and academia. In each of the three countries included above, the very nature of the shutdowns displayed the multiple actors required to exert control over access to the Internet. For example, the government could not drastically reduce the ability to communicate without the compliance of telecommunications companies, including Internet Service Providers. In each country, telecommunications companies complied with orders by government actors to

shut off access to the Internet, despite their responsibility to protect and promote human rights, and to provide secure and stable Internet access.[31] While the definition of the responsibility principle does not refer explicitly to international law, all actors are bound by international law, and David Kaye, former UN Special Rapporteur on Freedom of Expression, has stated that "a general network shutdown is in clear violation of international law and cannot be justified by any means".[32]

For example, in Uganda, telecom companies such as MTN, Airtel, and Africell all implemented government directives to block Internet access. In the DR Congo, telecom operators were asked by the regulator to restrict communications "In order to prevent the exchange of abusive images via social media by subscribers and to … take technical measures to restrict to a minimum the capacity to transmit images".[33] In Tanzania, telecom companies Viettel Tanzania, Vodacom Tanzania, and Tigo also immediately complied with government directives. On the other hand, Internet Service Providers in countries such as Lesotho and Gabon have pushed back against Internet shutdowns.[34] They questioned their intentionality, pointing out provisions in law that guarantee enjoyment of rights to freedom of expression, and engaged the government with support of civil society to maintain and defend uninterrupted Internet access and use.

A general network shutdown is in clear violation of international law and cannot be justified by any means.

As such, telecom companies can and should take the responsibility to resist government measures that undermine responsible behavior, and the government should not abuse their position of power in relation to other actors in the distributed ecosystem by ordering the shutdowns. As UN Special Rapporteur on the rights to freedom of peaceful assembly and of association, Clément N. Voule, has outlined in a recent report to the Human Rights Council, there are a range of measures that digital technology companies, including telecommunications providers and digital communications platforms, can undertake to ensure compliance with their human rights responsibilities even in light of business pressure and other limitations.[35]

The "Restraint" principle provides that no state or non-state actor should take actions that impair the stability of cyberspace. Each of the shutdowns in DR Congo, Tanzania, and Uganda disrupted all users' confidence in their ability to use cyberspace safely and securely, and meant that they could not be assured of the availability and integrity of services and information.

The GCSC also describes this principle as the expectation that both state and non-state actors "prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security." As the Internet Society has pointed out, "Internet users within a country experiencing a shutdown could lose access or experience reduced speed on interconnected networks if traffic needs to be routed through less optimal paths, resulting in collateral damage or systemic risks that go beyond a country's borders.[36] According to ISOC, "wide-scale Internet shutdowns can also have a detrimental impact on the domain name system (DNS),"[37] due to asymmetric DNS traffic requests that can result from shutdowns, which results in a surge in DNS requests and increased load on resolver infrastructure that can have collateral effects. Shutdowns that impact interconnection points or other significant infrastructure components could also impact connectivity and Internet performance in other countries, which could inadvertently harm international relations."[38] For example, "the outlawing of VPNs can severely inconvenience foreign diplomats and large companies which use them because they provide extra security."[39] In addition, if the country hosts services or platforms that are used outside the country, then users outside the country risk losing access to these services, platforms, or related applications. Global organizations op-

erating both within and outside the DR Congo, Tanzania, and Uganda would have been required to have their own platform in order to communicate freely with colleagues outside the country, or rely on VPNs. Yet, further research is required to understand whether or how these countries' shutdowns affected the DNS, connectivity, network resilience, and Internet performance in neighboring countries.[40]

The DR Congo shutdown did elicit diplomatic reaction, with the United States, Canadian, and Swiss heads of mission in Kinshasa urging the government to immediately restore communications,[41] while the EU condemned the 2021 shutdown in Uganda.[42] However, further research could also explore whether, by ordering the wide-scale blocking of texts and social media applications, including VPNs, these countries engaged in ICT practices that risked harming international relations by inconveniencing neighboring countries as well as foreign entities, including companies and diplomats within the country. It could also assess whether trust and relationships between ISPs are impacted, particularly as the Border Gateway Protocol (BGP) network, which routes global Internet traffic, relies on trust between operators, ISPs, and others who are required to withdraw from the network when ordered to shutdown Internet access in the case of complete blackouts.[43]

The third principle is "a Requirement to Act" or to take affirmative action to preserve the stability of cyberspace. The "Requirement to Act" principle requires that states and non-state actors take reasonable and appropriate steps to ensure the stability of cyberspace, as defined above. The framework provides examples of such actions such as upgrading hardware and software, implementing patching, etc. As noted above, shutdowns can undermine the stability and resilience of the Internet, although further research is needed to understand the impact on the infrastructure of the Internet of the Tanzania, DR Congo, and Uganda shutdowns.

Shutdowns that impact interconnection points or other significant infrastructure components could also impact connectivity and Internet performance in other countries, which could inadvertently harm international relations.

Yet, the widespread blocking of social media experienced by those in the DR Congo, Tanzania, and Uganda, and the "Internet blackouts" experienced in Uganda can be understood to be in direct opposition of the positive and proactive steps required to ensure the stability of cyberspace, that is, to ensure the ability to use cyberspace safely, securely, and where the integrity and availability of information is assured. While some companies, such as MTN Uganda, outlined plans to refund customers whose data plans expired during the 2021 shutdown, this falls far short of the steps that telecom companies can take in the face of shutdown orders, including the adoption of mitigation strategies, transparency measures such as the disclosure of all relevant information about shutdowns (e.g., preservation of orders or threats to disrupt networks), notification to users, including at the very least the provision of "regular updates about the services affected or restored, the steps they are taking to address the issue, and explanations after the fact," and the use of legal options for challenging requests, including litigation.[44]

As the GCSC's cyberstability framework states, "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." The impact of Internet shutdowns on human rights, including civil, political, economic, social, and cultural rights, has been widely documented. Authorities who block Internet access and social media fail to uphold their international human rights obligations, including those relating to the right to free expression, provided for under Article 19 of the International Covenant on Civil and Political Rights (ICCPR) and Article 9 of the African Charter on Human and People's

Rights, to which the DR Congo and Tanzania and are signatories. They also violate national laws, including the national constitution of each country.[45] The circumstances under which the shutdowns occurred reveal the intent to restrict rights to freedom of expression and information, and to interfere with the right to freedom of assembly and association, particularly during events such as elections, conflicts, or mass demonstrations.[46] The UN Special Rapporteur, Clement Voule, has noted that national security cannot be invoked as a rationale for blocking Internet access, when in an actual sense the very reason for deteriorating national security is the suppression of human rights itself.[47, 48] Furthermore, Principle 37 of the Declaration of Principles on Freedom of Expression and Access to Information in Africa (revised in 2019) provides that States must facilitate the rights to freedom of expression and access to information online and the means necessary to exercise these rights, and must recognize that universal, equitable, affordable, and meaningful access to the Internet is necessary for the realization of freedom of expression, access to information, and the exercise of other human rights.[49]

The circumstances under which the shutdowns occurred reveal the intent to restrict rights to freedom of expression and information, and to interfere with the right to freedom of assembly and association, particularly during events such as elections, conflicts, or mass demonstrations.

The same Declaration states that "States shall not engage in or condone any disruption of access to the Internet and other digital technologies for segments of the public or an entire population." In addition, the general comment No. 34 (2011) on the freedoms of opinion and expression, the Human Rights Committee, notes that Internet shutdowns are a disproportionate measure (generic bans on the operation of certain sites and systems are not compatible with paragraph 3).[50] The shutdowns, therefore, violated freedom of expression, access to information, and the right to peaceful assembly.

The impact of the Internet shutdowns in each country on human rights also affected economic, social, and cultural rights. The International Covenant on Economic, Social and Cultural Rights (ICESCR) defines a number of rights, including the free pursuit of his or her economic, social, and cultural development. The shutdowns in the DR Congo, Tanzania, and Uganda directly impacted these rights by vastly reducing the ability of millions of people in each country to trade, make money, and access a wide range of services, including educational and health services. The disruption to mobile services in Uganda impacted mobile money services, which are critical to both the formal and informal economies.

One example is a February 2021 report from the Daily Monitor: one of the leading newspaper dailies in Uganda notes that Internet shutdowns affected "key sectors of the economy such as trade, transport, banking, telecom, education, entertainment, media, health, and information technology support."[51] The same Daily Monitor report continued to assert that shutting down the Internet affected payment systems, Real Time Gross Transfers, and Electronic File Transfers. It stressed that "13,000 bank agents who conduct money transfers, Internet banking, and the Automatic Teller Machine"[52] were affected. According to the Internet Society, the cost of Internet shutdowns on the five-day shutdown in Uganda during the 2021 elections amounted to 9 million USD.[53] According to Jumia Uganda—an online shopping store—"cash reconciliation was very difficult because it relies on the Internet, and the whole supply chain suffered, resulting in a lack of access to food, medicines, and groceries."[54] The shutdown in the Democratic Republic of Congo in December 2018 is estimated to have cost the country 3 million USD.[55] In Tanzania, millions of people were unable to earn a livelihood; according to estimates, between 15–27% of young people's income is made

online in the country.[56] It's important to note that the increased dependence on the Internet as a result of the COVID-19 pandemic exacerbated the impact of the shutdown on all of these rights, as people became increasingly dependent on the Internet to carry out basic daily activities, including schooling/education, access to healthcare, transportation and other services.[57]

In addition, Uganda, Tanzania, and the DR Congo have all ratified the Convention on the Elimination of Discrimination against Women (CEDAW). Recent research demonstrates that shutdowns disproportionately impact women as a result of existing inequalities and more vulnerable positions in the economy and society, drawing on cases in India, Iran, Venezuela, and Pakistan.[58] This includes impacts to personal safety and professional and economic safety. However, research on the gender impact in other parts of the world that experience Internet shutdowns has been more limited to date. Further research on the impact of the shutdowns on women and the gender-differentiated impact of Internet shutdowns in the East Africa region would support a better understanding of how the rights of women and girls are affected by Internet shutdowns in different regions of the world.

Our preliminary assessment of the shutdowns in the DR Congo, Tanzania, and Uganda show that the shutdowns undermine the cyberstability framework, as these actions violate all four cyberstability principles; they can be seen as a detrimental effect on regional or national cyberstability overall. In particular, they impacted the human rights principle, a situation which was exacerbated by the increased reliance on digital technology during the COVID-pandemic in 2020. However, further research that captures more granular information about the impact of shutdowns, as recommended elsewhere by GNI, for example,[59] including its gendered impact, would support a greater understanding of the way that shutdowns impact the human rights principle of the cyberstability framework. This could build on work already done on the gendered impact in other countries and regions. The shutdowns impacted the "Responsibility," "Restraint," and "Requirement to Act" principles, particularly as they resulted in the inability of citizens to be able to use cyberspace safely, securely, and in a way where the integrity and availability of information is assured. Further research into how shutdowns impact the restraint principle should be further explored, including the impact on the DNS and on the resilience of networks/access in neighboring countries through collateral border effects. Further research could explore how shutdowns affect the GCSC norms, including, for example, the public core norm—particularly if sufficient evidentiary information on how shutdowns affect the DNS and network stability can be collected. This exploratory article has shown that shutdowns undermine the framework in different ways, and it has identified some gaps where further research would be helpful in forming a more detailed understanding of the relationship between cyberstability and Internet shutdowns. It is a first step and could be expanded to other countries in order to better understand the range of contexts in which shutdowns occur, the similarities between them, and their differences in relation to the GCSC's cyberstability framework.

Our preliminary assessment of the shutdowns in the DR Congo, Tanzania, and Uganda show that the shutdowns undermine the cyberstability framework, as these actions violate all four cyberstability principles; they can be seen as a detrimental effect on regional or national cyberstability overall.

Below we have drawn from the UN Special Rapporteur's comprehensive report on shutdowns and his recommendations, in particular, aligning his recommendations with the cyberstability principles.[60] We have also, where relevant from our analysis, provided some additional recommendations for each stakeholder group.

Recommendations

Responsibility

In order to uphold the principle of "Responsibility," civil society and academia should support companies in challenging unlawful shutdown orders, as well as work with other stakeholders to develop and socialize resources to help Internet users prepare for, prevent, and predict Internet shutdowns.

As stated in the most recent report by the UN Special Rapporteur on Rights to Freedom of Peaceful Assembly and of Association, governments should "ensure that the Internet, including social media and other digital communication platforms, remains open, accessible, and secure. Specifically...States should (i) order Internet Service Providers operating in their country to provide everyone with universal, affordable, high-quality, secure, and unrestricted Internet access throughout election periods, protests...And thereafter (iii) guarantee the safety of technical workers building and maintaining critical infrastructure networks, while ensuring sites are protected, and (iv) promote and protect strong encryption, including by adopting laws, regulations, and policies in line with international human rights, norms, and standards."[61]

Telecom companies and ISPs should take the responsibility to address government measures that undermine responsible behavior by promoting greater transparency.

Telecom companies and ISPs should take the responsibility to address government measures that undermine responsible behavior by promoting greater transparency. In line with the recommendations from the UN Special Rapporteur, they should disclose "information about the circumstances under which they may shut down the network, the demands they receive, and actions to push back on or mitigate the effects of government orders." Ahead of a shutdown, they should "provide timely and transparent guidance to users to identify disruptions likely to impact the quality of service they receive."[62] They should also publish transparency reports, notifying affected users and showing government requests and orders for network disruptions, as well as state their level of compliance to domestic and international laws.

Restraint

Limited publicly available evidentiary information exists on the impact of shutdowns on network stability, in particular how shutdowns may impact Internet speed in neighboring countries, and whether shutdowns that impact interconnection points or other significant infrastructure components have harmed relations in neighboring countries. Therefore, in order to uphold the principle of "Restraint," civil society and academia should work with actors in the technical community (including ISOC chapters, for example) to research the impact of shutdowns on the stability of the network, infrastructure components, the DNS, and Internet speed in neighboring countries, in order to better understand the impact of shutdowns on network availability more widely and on the Internet itself.[63]

As outlined in the aforementioned report of the UN Special Rapporteur, governments should "Refrain from shutting down, throttling, or blocking the Internet, and make a state pledge to refrain from imposing any unlawful restrictions on Internet access and telecommunication in the future, particularly in upcoming elections and protests, and amid the COVID-19 pandemic."[64]

Finally, telecom companies should "Challenge censorship and service limitation requests from states, using all available tools of law and policy, in procedure and practice,"[65] and explore oppor-

tunities to collaborate with civil society in doing so. They should also (along with civil society—as recommended above) collaborate to gather and publish granular information on the collateral impact of shutdowns on their networks and systems, including on their autonomous systems (ASes).

Requirement to Act

Civil society and academia continue to raise awareness of the impact of Internet shutdowns on people, the economy and human rights, including by collecting evidence, developing and sharing tools for documenting shutdowns, and advocating against them. They should continue to track the impact of Internet shutdowns, through the use of network measurement tools and other tracking skills—particularly in countries where there is a dearth of information available on shutdowns and their impact, e.g., the DR Congo.

Governments should proactively repeal and amend any laws and policies that allow for Internet shutdowns and enact legislation prohibiting and punishing these measures, as well as expand initiatives to provide universal and affordable Internet access.[66]

Telecom companies should "engage regulators and push back against licensing conditions (and laws governing the telecommunications sectors) that allow for shutdowns," and, where they are required to comply with shutdown orders, they should "establish response plans and channels of communication with government actors and civil society."[67] They should also "prepare for a range of threats to the rights of users, particularly where bandwidth is overwhelmed and congested as a result of large demonstrations, and ensure that the company deploys extra capacity throughout the events."[68]

Human Rights

Civil society should generate and use evidence-based data to raise awareness and stimulate discussions and debates that inform public policy across all stakeholder groups about the negative impact of Internet shutdowns on human rights, including where there is more limited information, such as on the gendered impacts of Internet shutdowns in the Africa region.

States have obligations under international human rights law to ensure that everyone within their jurisdiction is able to access and use the Internet to exercise their human rights. In line with the recommendations in the UN Special Rapporteur's report, therefore, they should "recognize the right to access and use the Internet as a constitutional and legal right and as an essential condition for the exercise of the right to freedom of peaceful assembly." They should also institute oversight mechanisms, ensuring all network disruptions are subject to detailed reports that are publicly accessible, which detail the nature and causes of the disruptions and assess legal compliance.[69]

Telecom companies should develop and make publicly available policies that specifically state their position against Internet shutdowns and how they address any shutdown orders from governments, in compliance with the UN Guiding Principles on Business and Human Rights.

Acknowledgements

The authors would like to extend their sincere thanks to Ashnah Kalemera (CIPESA) for her review and feedback, and to Nazar Nicholas (ISOC Tanzania) for the fact-checking and guidance he provided.

Endnotes

1 "Advancing Cyberstability," Global Commission on the Stability of Cyberspace. Accessed August 4, 2021. https://cyberstability.org/report/

2 KeepItOn: Frequently Asked Questions. https://www.accessnow.org/keepiton-faq/ Accessed August 4 2021.

3 E. Marchant and N. Stremlau, (2019). Africa's Internet Shutdowns: A report on the Johannesburg Workshop. Programme in Comparative Media Law and Policy (PCMLP), University of Oxford, http://pcmlp.socleg.ox.ac.uk/wp-content/uploads/2019/10/Internet-Shutdown-Workshop-Report-171019.pdf

4 State of Internet Freedom. Democratic Republic of The Congo 2019. Mapping Trends in Government Intent Controls 1999–2019. https://cipesa.org/?wpfb_dl=408. Accessed July 4, 2020.

5 The Evolution of Internet Shutdown in DR Congo. CIPESA. https://cipesa.org/2017/03/the-evolution-of-internet-shutdowns-in-dr-congo/

6 DR Congo Internet restored after 20-day suspension over elections. Accessed August 4, 2021. https://www.aljazeera.com/news/2019/1/20/dr-congo-internet-restored-after-20-day-suspension-over-elections

7 State of Internet Freedom: Democratic Republic of Congo 2019. Mapping Trends in Government Internet Controls, 1999–2019. Accessed August 26, 2021 https://cipesa.org/?wpfb_dl=408

8 Navigating Litigation During Internet Shutdowns in Southern Africa (2019). Accessed August 26, 2021. https://www.southernafricalitigationcentre.org/wp-content/uploads/2019/08/SALC-Internet-Shutdown-Guide-FINAL.pdf

9 Violating International Law, DRC Orders Telcos to Cease Communications Services (2018). Accessed August 25, 2021. https://www.accessnow.org/violating-international-law-drc-orders-telcos-vodafone-millicon-airtel/

10 Navigating Litigation During Internet Shutdowns in Southern Africa (2019). Accessed August 26, 2021. https://www.southernafricalitigationcentre.org/wp-content/uploads/2019/08/SALC-Internet-Shutdown-Guide-FINAL.pdf

11 Disruptions to Digital Communications Persists in the Democratic Republic of Congo (2018). Edrin Wanyama. Accessed August 23, 2021. https://cipesa.org/2018/01/disruptions-to-digital-communications-persist-in-the-democratic-republic-of-congo/

12 Navigating Litigation During Internet Shutdowns in Southern Africa. 2019. Accessed August 26, 2021. https://www.southernafricalitigationcentre.org/wp-content/uploads/2019/08/SALC-Internet-Shutdown-Guide-FINAL.pdf

13 "Internet penetration rate in Tanzania from 2015 to 2020." Accessed August 4, 2021. https://www.statista.com/statistics/1226024/internet-penetration-rate-in-tanzania/

14 "Internet disrupted in Tanzania on eve of general elections." October 27, 2020. https://netblocks.org/reports/internet-disrupted-in-tanzania-on-eve-of-presidential-elections-oy9abny3

15 "Directive on Temporal Suspension of Bulk Messaging and Bulk Voice Calling Services," October 21, 2020. https://www.accessnow.org/cms/assets/uploads/2020/10/TCRA-Directive-to-telcos-in-TZ-to-filter-content.jpeg

16 "Tanzania's Internet restrictions during election are 'despicable,' digital rights activist says." October 28, 2020. https://www.pri.org/stories/2020-10-28/tanzanias-internet-restrictions-during-election-are-despicable-digital-rights

17 Ibid.

18 "As Long as I am Quiet, I am Safe: Threats to Independent Media and Civil Society in Tanzania." Human Rights Watch. October 28, 2019. https://www.hrw.org/report/2019/10/28/long-i-am-quiet-i-am-safe/threats-independent-media-and-civil-society-tanzania

19 "Tanzania's internet restrictions during election are 'despicable,' digital rights activist says". October 28, 2020. https://www.pri.org/stories/2020-10-28/tanzanias-internet-restrictions-during-election-are-despicable-digital-rights

20 "Tanzania: Internet slowdown comes at a high cost" Accessed August 4, 2021. https://www.dw.com/en/tanzania-internet-slowdown-comes-at-a-high-cost/a-55512732

21 Ibid.

22 "Tanzania is weaponizing Internet shutdowns. Here's what its people have to say." December 16, 2020. https://www.accessnow.org/tanzania-internet-shutdowns-victim-stories/

23 Uganda Bureau of Statistics (2020). Highlighting Population Issues Through Statistics. Uganda Bureau of Statistics. Accessed July 5, 2021. https://www.ubos.org/wp-content/uploads/publications/07_2020WORLD-POPULATION-DAY-BROCHURE-2020.pdf

24 Uganda Communications Commission (2020). Market Performance Report 3 Q20. Uganda Communications Commission. Accessed July 5, 2021. https://www.ucc.co.ug/wp-content/uploads/2021/01/MARKET-PERFOMANCE-REPORT-Q3-2020-Final-compressed.pdf

25 Aljazeera (2021). Museveni declared winner of disputed Uganda presidential election. https://www.aljazeera.com/news/2021/1/16/ugandas-museveni-declared-winner-of-presidential-election

26 Accessnow (2018). Time is up: Uganda in Court over internet shutdowns that violate human rights. Accessed July 17, 2021. https://www.accessnow.org/uganda-in-court-over-internet-shutdowns/

27 Ibid.

28 Daily Monitor (2018). Government moves to block VPN as Ugandans vow to dodge social media tax. https://www.monitor.co.ug/uganda/news/national/government-moves-to-block-vpn-as-ugandans-vow-to-dodge-social-media-tax-1765758

29 Assessing the impact of social media on political communication and civic engagement in Uganda. Konrad Adenauer Stiftung. https://www.kas.de/c/document_library/get_file?uuid=95eec5bf-c11c-c4eb-f504-90a4e5a4d54d&groupId=252038

30 Switching off the Internet has a huge cost; it must never happen again. Daily Monitor. https://www.monitor.co.ug/uganda/business/prosper/shutting-the-internet-must-never-happen-again--3277616

31 Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework. https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

32 DR Congo: Restore Internet services as "a matter of urgency," urges UN expert. United Nations. Accessed on July 6, 2021. https://news.un.org/en/story/2019/01/1029952

33 Patient Ligodi, Congo orders Internet slowdown to restrict social media: telecoms source. https://tinyurl.com/rlrvf8d

34 How Telecom Companies in Africa Can Respond better to Internet disruptions. CIPESA. Accessed online June 26, 2021. https://cipesa.org/?wpfb_dl=435

35 "Ending Internet shutdowns: a path forward: Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association." June 15, 2021. A/HRC/47/24/Add.2. https://undocs.org/A/HRC/47/24/Add.2

36 "Internet Society Position on Internet Shutdowns." December 17, 2019. https://www.internetsociety.org/resources/doc/2019/internet-society-position-on-internet-shutdowns/

37 Policy Brief: Internet Shutdowns. Internet Society. https://www.internetsociety.org/policybriefs/internet-shutdowns/#_edn17

38 Ibid.

39 "Africa Internet: Where and How Are Governments Blocking it," January 14, 2021. https://www.bbc.co.uk/news/world-africa-47734843

40 Ibid. Regarding access in neighboring countries, a local ISOC representative in Tanzania said that neighboring countries, including Kenya, did not seem to be affected. However, asymmetric disruptions to DNS are not more likely to affect a geographic neighbor than they are a "network neighbour." This is especially the case when the shutdown impacts general Top Level Domains, for instance, those registered under .com. In such a scenario, it is possible that a local Internet in Africa could have some global effects. More research is urgently needed.

41 "DR Congo: Internet, SMS shutdown threatens credibility of election" https://www.dw.com/en/dr-congo-internet-sms-shutdown-threatens-crediblity-of-election/a-46917740

42 EU Condemns Internet Shutdown, Security Excesses as Uganda Votes. January 20, 2021. https://ugandaradionetwork.net/story/eu-condemns-internet-shutdown-security-excesses-as-uganda-votes-

43 "A Human Rights Based Approach to Network Disruptions" https://globalnetworkinitiative.org/wp-content/uploads/2018/06/Disconnected-Report-Network-Disruptions.pdf

44 "Ending Internet shutdowns: a path forward: Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association." June 15, 2021. A/HRC/47/24/Add.2. https://undocs.org/A/HRC/47/24/Add.2

45 Article 29 of the Constitution of Uganda provides for protection of freedom of expression, assembly, and association. Articles 23–25 of the Congo's Constitution guarantee citizens the right to freedom of expression, assembly, and association. See: https://cepa.or.ug/wp-content/uploads/2018/06/300460141-ARTICLE-29-THREATENED-A-CRITICAL-DISSECTION-OF-VARIOUS-LAWS-PASSED-THAT-UNDERMINE-FUNDAMENTAL-FREEDOMS-OF-SPEECH-EXPRESSION-ASSEMBLY.pdf ; https://cipesa.org/?wpfb_dl=234

46 Internet shutdowns and elections handbook. A guide for election observers, embassies, activists, and journalists. Accessnow. Accessed July 2, 2021. https://www.accessnow.org/internet-shutdowns-and-elections-handbook/

47 "Ending Internet shutdowns: a path forward: Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association". June 15, 2021. A/HRC/47/24/Add.2. https://undocs.org/A/HRC/47/24/Add.2

48 Uganda: Authorities must lift social media block amid crackdown ahead of election. Amnesty. Accessed online June 24, 2021. https://www.amnesty.org/en/latest/news/2021/01/uganda-authorities-must-lift-social-media-block-amid-crackdown-ahead-of-election/

49 Statement: Internet Shutdowns in Uganda Erode Citizen's Enjoyment of Basic Human Rights. Global Network Initiative. Accessed June 20, 2020. https://globalnetworkinitiative.org/concerns-internet-shutdowns-uganda/

50 Human Rights Committee, general comment No. 34 (2011), para. 43.

51 How internet shutdown stalled businesses. Daily Monitor. https://www.monitor.co.ug/uganda/news/national/how-internet-shutdown-stalled-businesses-3287376

52 How internet shutdown stalled businesses. Daily Monitor. https://www.monitor.co.ug/uganda/news/national/how-internet-shutdown-stalled-businesses-3287376

53 The Cost of Internet Shutdowns: Uganda, January 2021. Internet Society Pulse. https://pulse.internetsociety.org/blog/5026

54 Ibid.

55 Policy Brief: Internet Shutdowns. Internet Society. https://www.internetsociety.org/policybriefs/internet-shutdowns/#_edn17

56 "Tanzania: Internet slowdown comes at a high cost." Accessed August 4, 2021. https://www.dw.com/en/tanzania-internet-slowdown-comes-at-a-high-cost/a-55512732

57 "Ending Internet shutdowns: a path forward: Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association." June 15, 2021. A/HRC/47/24/Add.2. https://undocs.org/A/HRC/47/24/Add.2

58 "Assessing the Gendered Impact of Internet Shutdowns," presented by Sarah Shoker (2020). https://konnect.serene-risc.ca/2021/03/11/assessing-the-gendered-impact-of-internet-shutdowns/

59 J. Rydzak, Disconnected: A Human-Rights Based Approach to Network Disruptions (2018). Global Network Initiative. https://globalnetworkinitiative.org/wp-content/uploads/2018/06/Disconnected-Report-Network-Disruptions.pdf. Accessed August 4, 2021.

60 "Ending Internet shutdowns: a path forward: Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association". June 15, 2021. A/HRC/47/24/Add.2. https://undocs.org/A/HRC/47/24/Add.2

61 Ibid.

62 Ibid.

63 Ibid.

64 Ibid.

65 Ibid.

66 Ibid.

67 Ibid.

68 Ibid.

69 Ibid.

About the Authors

Moses Owiny is the Founder and Chief Executive Officer at the Centre for Multilateral Affairs (CfMA) in Uganda. The CfMA is a platform that seeks to aid policy thinking as well as contribute to research and the body of knowledge, integrating Global South perspectives in domestic, regional, and global policy discourses. His recent research work in Uganda focused on cybersecurity and state capacity. In June 2021, he served as an external co-chair and Programme Committee member for the 10th edition of RightsCon under the category "Cyber Norms, Accountability, and Practice."

Sheetal Kumar currently provides strategic oversight for a global cybersecurity capacity-building programme that supports civil society organizations from the Global South, to protect and promote human rights in cybersecurity- and cybercrime-related discussions. She also facilitates civil society engagement in key relevant forums, including the UN, through research, facilitation, and coordination support on a day-to-day basis. Her recent work has focused on applying human-centric approaches to cyber policy, including cyber norms.

Cyberstability Paper Series

New Conditions and Constellations in Cyber

Digital Transformation and Cyberstability: Effects on Economic Development in Africa

Prof Bitange Ndemo
Professor of Entrepreneurship at the University of Nairobi

Digital Transformation and Cyberstability: Effects on Economic Development in Africa

Prof Bitange Ndemo | Professor of Entrepreneurship at the University of Nairobi

Since 2009, Africa has made significant investments in digitalization (a process of converting information from analogue to digital form). Owing to this conversion, the continent now leads the world in the digitalization of currency (i.e., mobile money). Many countries have integrated the Fourth Industrial Revolution (4IR) technologies into the center of the continent's economic development, and, in doing so, these nations have forced a consideration of whether digitalization could potentially become the driver of economic growth. Should digitalization happen to play this role, Africa's developing countries (highly informal agrarian societies wherein industrialization, in the classic sense, never occurred) could leapfrog stages of classic industrial development and thereby birth a new model of change. However, as digitalization increasingly drives economies, cybersecurity solutions will become necessary.[1] This paper highlights Africa's digitalization process and points to cyberstability as essential for the continent's short- and long-term economic development and sustainability.

Structural change in Africa has been largely underpinned by digitalization, agro-industries, and the evolution of the global marketplace. Those "industries without smokestacks"[2] that are the products of this structural change have arisen in contradiction of Arthur Lewis's theory of growth, which postulated that a "capitalist" sector developed by taking labor from a non-capitalist, backward "subsistence" counterpart.[3] More specifically, for Lewis, development occurred when labor moved from an unproductive informal sector (e.g., subsistence farming and small trade) to a productive formal one (e.g., large manufacturing). Lewis's theory has been borne out, for the most part, in developed

Bitange Ndemo is Professor of Entrepreneurship at the University of Nairobi. His research centers on the link between ICTs and SMEs with emphasis on how ICTs influence economic development in Africa.

countries where labor-intensive manufacturing enterprises have absorbed those workers shifting from low wages in agriculture and other informal activities amid the information age.

The author's own experience in shaping most African countries' digitalization policies between 2006 and 2013 bear on this question. As several countries on the continent initiated plans to develop information and communication technology (ICT) infrastructure (e.g., undersea cables), the individuals who had been highly involved in that process imagined these emerging technologies could act as a "bridge" toward industrialization and the services economy. At that time, the continents' governments' policy goals sought to leverage the growing gig economy to provide employment for Africa's burgeoning population. Those involved at this early stage expected digitalization to encourage increased productivity while transforming ailing national economies, even as this anticipation was not supported by evidence.

The urge to digitalize the continent was inspired by the author's meeting with Thomas Friedman, the former New York Times columnist and author of the best-selling book The World is Flat.[4] During that meeting, Friedman explained how India took advantage of cheap undersea fiber-optic networks and abundant labor to create massive employment for those in the business process outsourcing (BPO) industry. But Friedman also stressed that Africa could do the same thing, thereby sowing a seed that would change the economic fortunes of the continent. After meeting with Friedman, the author shared the columnist's widely read and highly influential book with other policymakers and advocated digitalization during every speaking opportunity, especially at the International Telecommunication Union (ITU) policymakers' meetings, which were focused on investments in digital infrastructure and digitalization.

Within years of that meeting and owing to policy developments across the continent that had been initiated during the preceding decade, change was afoot. By 2012, a World Bank study noted that the ICT sector had "been the major economic driver in Sub-Saharan Africa over the past decade."[5] The same study also indicated that, while mobile and internet penetration remained comparatively low in Africa, "never before in the history of the continent has the population been as connected as it is today."[6] Empirical evidence on the relationship between digitalization and its economic impact on, for example, productivity,[7] manufacturing,[8] and job creation,[9] has validated the assumptions of the author and others many years ago when the establishment of a digital infrastructure was first being considered.

In a similar vein, FinTechs (digitalized financial services) have challenged traditional financial structures—bringing greater inclusivity and efficiency in certain economies. The prevalence of FinTechs has been pronounced on the continent to such an extent that, as the International Monetary Fund noted, "Sub-Saharan Africa has become the global leader in mobile money transfer services, spurring widespread access to financial services."[10] Indeed, the IMF report went on to say, while "Sub-Saharan Africa has lagged behind the rest of the world in access to finance, some countries in the region are now global leaders."[11] FinTechs continue to transform financial access in Africa, catalyzing other sectors, such as micro-enterprises and agriculture.

And yet, owing to this increased digitalization and heightened connectivity between developing countries, Africa has also seen both increasing amounts of cybercrime and more frequent cyber-attacks.[12] The space has essentially become a kind of "magnet" for cybercriminals, thereby necessitating attention to cybersecurity and underscoring the need for cyberstability. The rest of this paper will, therefore, attend to the following questions: To what extent has Africa digitalized? And: How can cyberstability sustain this process and encourage greater prosperity on the continent?

These questions will be addressed through a discussion of the drivers and indicators of digitalization, a review of the primary barriers to digitalization on the continent, and an assessment of the relationship between digitalization and cyberstability. Overall, this paper points to gaps warranting further investigation in the field, highlights progress that has been made and growth that has yet to be realized, and makes the case for a continent-wide commitment to the kinds of development already realized by certain of Africa's leading and most digitized nations—countries that were early adopters of digitalization.

Because there is no uniform definition of digitalization, the concept will, in this paper, refer to the leveraging of digital technologies, such as mobile telephony, broadband, and cloud computing to create, process, transmit, and analyze in a digital fashion[13] In this way, digitalization helps create new business models and value-producing opportunities, while also improving productivity—all of which are essential for economic development.

As this paper will argue, Africa's digitalization process is best understood in light of Everett Rogers's Diffusion of Innovation (DOI) theory, a notion that addressed why new ideas are never simultaneously accepted by all people.[14] While digitalization has been adopted by some countries on the continent, for example, others are still going through a process of acceptance that has been—and will continue to be—influenced by many factors. This is because different social systems include their own response times. For example, the ubiquity of mobile money in Kenya has not translated to acceptability in South Africa, a market with a different income stratification. It is also worth noting that certain countries have been inclined to move toward digitalization as early adopters, while others have come along as the early majority, the late majority, or as laggards.

While degrees of digitalization vary, therefore, according to myriad influences, it is possible to measure levels of digitalization by different types of indicators. The more common measures are provided by the ITU, which mainly focuses on ICTs, including access to infrastructure, such as broadband, as well as electricity calculated as a percentage of use if individuals (including their skill levels) are using internet or electricity. But indicators may also include quality—that is, internet bandwidth per user—as well as access to devices such as fixed telephones and mobile phones. In other cases, measures of digitalization extend to how institutions such as enterprises, education, and government utilize ICTs. For the purposes of this paper, indicators of digitalization will, thus, include access, skills, and use,[15] all of which lead to product innovations and improved decision-making for economic transformation.

Although internet penetration today is 40%, a 10% increase in mobile-internet penetration can increase GDP per capita by 2.5% in Africa, as opposed to only 2% for the rest of the world.

Investment in undersea and terrestrial fiber-optic lines led to rapid growth in international internet capacity and narrowed the access gap in most countries, with the exception of, for example, the Central African Republic and Somalia, where internal war inhibited development. Last-mile 4G mobile-technology coverage for the continent averages about 50%, with Central and West Africa averaging 41%. Slightly over 50% of the population have mobile phone subscriptions, and at least 45% use smartphones. Nigeria, South Africa, and Kenya are the top three smartphone markets; so, too, are these three countries the top developers of apps, with extensive digitalization of both their public and private sectors.[16] A recent International Finance Corporation (IFC) study showed that, although internet penetration today is 40%, a 10% increase in mobile-internet penetration can increase GDP per capita by 2.5% in Africa, as opposed to only 2% for the rest of the world. What this means is that increasing internet penetration to 75% by 2025, as has been envisaged, could create 44 million

new jobs.[17] Finally, investments in solar-energy solutions are paying off; over 640 million, or 40% of Africans, are currently connected to this source of energy.[18] Although the average energy connectivity rate is still somewhat low, progress has been made, and many countries enjoy coverage at a rate exceeding 70%.

Skills development is also a major component of digitalization. In the past ten years, the literacy rate in Africa has jumped from 58%, in 2010, to nearly 67%, in 2019.[19] Moreover, secondary school enrollment surged between 2000 and 2018, climbing from 25% of gross enrollment to 43%, whereas the world average in 2018 was 66%. Finally, and most apt for the purposes of this paper, at least 50% of African countries (compared to 85% for the world at large) have launched digital-literacy programs to enable individuals to interface with digital-learning programs, while, at the same time, making institutional reforms to deliver and maintain digital content for learning purposes.[20] The pandemic that began in 2020 and the surge of COVID-19 cases actually helped in this regard: nations began to fast track their adoption of digital-learning options in virtually all higher- and lower-level educational institutions.

All this said, those governments which have embraced digitalization of services have seen the dividends of using ICTs. For instance, in Algeria, Egypt, Ghana, Kenya, Nigeria, Morocco, South Africa, and Tanzania, digital technology has driven innovation, spurred economic growth, and encouraged job creation in many key sectors of the economy. These sectors have included agriculture, health, education, and financial services.[21] Institutions of higher learning in these countries were, as a result, better prepared to absorb the impact of the pandemic and were well-positioned to pivot into remote teaching and learning.

Local digital innovations, another measure of digital capability, is expanding in Africa. The number of startups has grown, as has the amount of money they have the potential to attract. Indeed, from 2015 to 2020, the number of startups that secured funding shot up from 55 to 375,[22] while the total amount of money they raised climbed from $400 million to $2 billion during roughly the same period (2015–2019).[23] Even during 2020, a year colored so profoundly by the pandemic, startups managed to raise $1.43 billion.[24]

Funded startups can be found across Africa, but four countries—Kenya, Nigeria, South Africa, and Egypt (sometimes referred to as the Big Four)—accounted for 77% of these startups and 89.2% of total investment in 2020.[25] In the same regard, these four nations claim about 50% of the nearly 700,000 professional developers on the continent. The Big Four countries are set apart from others in Africa due to a good inventory of digital skills, a reasonable ICT infrastructure, and institutionalized cybersecurity.

Another characteristic distinguishing the Big Four from neighboring nations is that they are regionally dominant. For example, in East Africa, Kenya's economy is larger and well-diversified, while Egypt dominates North Africa. Nigeria and South Africa, for their part, are the dominant economies in Western and Southern Africa, respectively. Early adoption, in the sense imagined by Rogers and as discussed above, means being willing to accept occasional setbacks (accommodating risk), especially when new ideas prove unsuccessful.[26] These countries have great influence on their neighboring nations, or those within the same trading bloc, and they have swayed nations like Algeria, Ghana, Morocco, and Tanzania to seed more of their own local innovations and enterprise. The innovation space is large in a continent with so many problems, meaning there is less competition between frontrunners and followers.

Given that most countries have invested in enabling infrastructure, that the use of ICTs is growing, that more young people are completing high school and a good number are completing college, and that the number of incubation hubs is increasing in virtually every African country, the continent is on path to witness, in the near future, the early majority period of entry spelled out by Rogers in his DOI theory. For this to happen, African countries must invest heavily in ICT skills, infrastructure, and cyberstability; so, too, must the continent's nations encourage use of digitalization across all sectors of the economy, in the spirit of the African Union's call for all member states to model the increased inclusivity that arose in the FinTech sector. In general, Africa has made significant gains in the way of digitalization, as indicated by conventional metrics, and these data and examples show that the continent is on track to close the gap that currently exists vis-à-vis the rest of the world.

The primary barriers to digitalization on the African continent include weak educational systems in most nations, political intolerance of social-media freedoms, the difficulty of managing a rapidly changing technological environment, challenges associated with building an enabling regulatory environment to support disruptive startups, and the uneven distribution of infrastructure investment in rural and urban centers.

Africa has long been under pressure to increase enrollment in its education systems. Yet such an increase invites its own consequences—some foreseen, some not. For example, enrollment that grows without a commensurate increase in training programs, or quality control standards, can lead to inequality and exclusion within an educational system.[27] In other words, "more education" does not necessarily mean that "more" are "educated," at least in a fashion that is consistent and equitable across or even within countries. Factors such as high repetition rates, teacher shortages, untrained instructors, poor school management, and underperformance in examinations can individually and collectively diminish the quality of available education on the continent. Additionally, the shortage of technical skills across Africa, where less than 10% of tertiary students are studying science, technology, engineering, or mathematics (the STEM fields), as well as outdated curriculums and inadequate materials significantly inhibit digitalization on the continent.[28]

The primary barriers to digitalization on the African continent include weak educational systems in most nations, political intolerance of social-media freedoms, the difficulty of managing a rapidly changing technological environment, challenges associated with building an enabling regulatory environment to support disruptive startups, and the uneven distribution of infrastructure investment in rural and urban centers.

Political intolerance in some African governments has also affected the use of ICTs, especially when state officials shut down the internet at the slightest provocation in social media. Such comparatively intolerant governments have included those of Burundi, Cameroon, Chad, Ethiopia, Guinea, Mali, Sudan, Togo, Uganda, and Zimbabwe. Other governments have undermined the use of ICTs by regularly taxing devices and broadband use to limit the effectiveness of these options. The pace of innovation in the several hubs spread across the continent has grown tremendously, but regulators across the continent are becoming a barrier, often seeking to regulate even those innovations that pose no threat to consumers. These regulatory threats are increasingly pushing developers toward countries with a more enabling policy environment, such as Kenya, for example, where the author chaired the task force that developed the roadmap for blockchain and artificial intelligence. That task force recommended legal sandboxes to enable innovators to test their products under the watchful eyes of regulators, and its final report has been shared in many other African countries.

Finally, according to a report by the ITU, which measured digital development, only 44.3% of the continent's population has access to 4G coverage, compared to 82.3% of people living in other developing countries.[29] This discrepancy is due, primarily, to the fact that 4G access favors urban dwellers. Only 22% of those living in rural areas enjoy such opportunities, for example, compared to 77% of those inhabiting cities—a distinction that owes much to heavy taxes on broadband. Closing this gap will require policies finely tuned to the particular needs of the continent, with co-operation between government and industry of a kind that can best address the needs of nations with willing users but without the infrastructure, environment, or enabling institutions evident in other parts of the world.

For the Global Commission on the Stability of Cyberspace (GCSC), stability with respect to cyberspace refers to a state where "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."[30] Cyberstability has, thus, become a major topic of discussion in Africa; many countries have realized that, as organizations digitize enterprises and automate operations, the incurred risks of digitalization will multiply.[31] In this regard, a 2020 study by the Kaspersky group concluded that, while Africa has the same hit rate as other parts of the world when it comes to cyberattacks and activity,[32] the continent registered a significant increase in financial/banking cybercrimes in the second quarter of 2021 when compared to figures for the first quarter in 2021. In particular, the report noted a 59% increase in cybercrimes in Kenya and a 32% increase in the same behavior in Nigeria.[33] Not surprisingly, these nations have led the continent in terms of digitalized currency and are two members of the Big Four countries discussed above.

Encouraging greater and more widespread cyberstability depends on many factors. The ITU developed an index to aid in this effort, known as the Global Cybersecurity Agenda (GCA). This index assessed each country on the continent according to five strategic pillars (legal measures, technical measures, organizational measures, capacity building, and international cooperation). The ITU then used this organizational scheme to gather data and aggregate an overall score, with the Union's 2019–2020 assessment reflecting data and conditions amid the Covid-19 pandemic. By the measures of this report then, the top ten African countries most committed to cyberstability were, with their overall scores in parentheses, Mauritius (96.89), Tanzania (90.58), Ghana (86.69), Nigeria (84.76), Kenya (81.7), Benin (80.06), Rwanda (79.95), South Africa (78.46), Uganda (69.98), and Zambia (68.88).[34] It is notable that Mauritius, with a score of 96.89, scored almost as well as India, which registered a 97.5 and which ranked tenth overall in the world.[35]

Not surprisingly, many of the ten African countries most committed to resolving the issue of cybersecurity were the same ones who had been in the forefront of establishing an institutional framework, enabling ICT infrastructure access to citizens, intensifying the use of ICTs in all aspects of the economy, and bolstering relatively developed ICT skills. By contrast, and reflecting the relative lack of preparedness of many other nations, only eighteen African countries currently have an institutional framework for reporting cybersecurity incidents through their respective National Computer Security Incident Response Teams (CSIRTs). In the same regard, the African Union, during its 2019 meeting, noted Africa's advances in digitalizing its economies and acknowledged the challenges the continent faces, including the gap among AU member states in terms of the awareness, knowledge, understanding, and capacity to adopt and deploy the proper strategies, capabilities, and programs to mitigate cyber threats.[36] Statistics such as these point to both what is possible and how much work must still be done to position countries across the continent to embrace the progress that can come through digitalization.

Conclusion

Over the past ten years, the author has traveled to more than thirty-five African countries to share his experience in policymaking and to speak to the impact of emerging technologies. The message conveyed through these engagements has been simple and direct: one should not fear something one has not tried. Africa must learn from prior industrial revolutions, embrace change, and find its role in the 4IR. The sustainability of enterprises in the digital age is underpinned by the adoption of innovation and digital changes, as a strategy for improving the efficiency and performance of organizations.[37] Eventually, such digital exposure will lead to digital disasters or disruptions, both of which require cybersecurity.[38]

Digital transformation, cyberstability, and economic development are critical subjects for a continent aiming to integrate 55 economies into a single market. While the Big Four nations have seen the most benefit—and have benefited the longest—from digitalization, countries such as Algeria, Ghana, Morocco, and Tanzania are closing the gap. Returning to Rogers's DOI theory then, around which this paper's argument has been centered, Africa has seen both early adopters and an early majority. For the continent to fully exploit digitalization in this emerging 4IR, it must embark on human-resource development to ensure it can retain (or establish) the skills required to sustain economies. So, too, must countries carefully consider their use of taxes on broadband and related devices—tactics that could be frustrating ICT use when precisely the opposite approach is called for and much overdue.

For the continent to fully exploit digitalization in this emerging 4IR, it must embark on human-resource development to ensure it can retain (or establish) the skills required to sustain economies.

Moreover, countries are urged to reevaluate arguably outdated cultural and religious practices that prevent women—more than half the population—from productively participating in the economy. Reforms are especially important during this critical period of the 4IR, which offers the opportunity to reinvigorate manufacturing and help various economies expand their employment opportunities. Further, the continent must ensure access to a supporting infrastructure (broadband and energy) and must also work to make devices and access affordable. Finally, if the continent is to benefit from its innovations, regulatory regimes should create an enabling environment. One cannot reap what one has not been allowed to sow. Africa's past is instructive but need not be limiting; its future depends perhaps more than ever on choices made in the present.

Endnotes

1 World Bank, "World Bank and Partners Announce New Global Fund for Cybersecurity," Press Release, August 16, 2021, https://www.worldbank.org/en/news/press-release/2021/08/16/world-bank-and-partners-announce-new-global-fund-for-cybersecurity.

2 Richard Newfarmer, John Page, and Finn Tarp, eds. Industries Without Smokestacks: Industrialization in Africa Reconsidered (Helsinki: UNU-WIDER, 2018), http://fdslive.oup.com/www.oup.com/academic/pdf/openaccess/9780198821885.pdf.

3 Arthur Lewis, "Economic Development with Unlimited Supplies of Labour," The Manchester School 22, no. 2 (1954): 139–191, https://doi.org/10.1111/j.1467-9957.1954.tb00021.x.

4 Thomas Friedman, The World is Flat: A Brief History of the Twenty-first Century (New York: Macmillan, 2005).

5 Javier Ewing et al., ICT Competitiveness in Africa (Washington, DC: World Bank, 2014), https://openknowledge.worldbank.org/handle/10986/19025 License: CC BY 3.0 IGO.

6 Ewing et al., ICT Competitiveness in Africa.

7 OECD, "Digitalisation and Productivity: A Story of Complementarities," Economic Outlook 2019, issue 1 (2019), https://www.oecd.org/economy/outlook/digitalisation-and-productivity-complementarities/.

8 Rafael Lorenz et al., "Digitalization of Manufacturing: The Role of External Search," International Journal of Operations & Production Management 40, no. 7/8 (2020), https://doi.org/10.1108/IJOPM-06-2019-0498.

9 Jieun Choi, Mark Dutz, and Zainab Usman, The Future of Work in Africa: Harnessing the Potential of Digital Technologies (Washington, DC: World Bank, 2020), http://hdl.handle.net/10986/32124.

10 International Monetary Fund, FinTech in Sub-Saharan African Countries: A Game Changer? No. 19/04 (Washington, DC: IMF Publication Services, 2018), p. vii, https://www.imf.org/-/media/Files/Publications/DP/2019/English/FTSSACEA.ashx.

11 International Monetary Fund, FinTech in Sub-Saharan African Countries.

12 Niels Nagelhaus Schia, "The Cyber Frontier and Digital Pitfalls in the Global South," Third World Quarterly 39, issue 5 (2018): 821–37, https://doi.org/10.1080/01436597.2017.1408403.

13 World Bank, World Development Report 2016: Digital Dividends (Washington, DC: World Bank, 2016), doi:10.1596/978-1-4648-0671-1.

14 Everett Rogers, Diffusion of Innovations (Free Press of Glencoe, 1962).

15 International Telecommunication Union Secretariat, "ICT Development Index: A Proposal," September 2020, https://www.itu.int/en/ITU-D/Statistics/Documents/events/egti2020/IDI2020_BackgroundDocument_20200903.pdf.

16 GSMA, The State of Mobile Internet Connectivity 2020 (London: GSMA Head Office, 2020), https://www.gsma.com/r/wp-content/uploads/2020/09/GSMA-State-of-Mobile-Internet-Connectivity-Report-2020.pdf.

17 International Finance Corporation, "e-Conomy Africa 2020: Africa's $180 Billion Internet Economy Future," World Bank Group, https://www.ifc.org/wps/wcm/connect/6a940ebd-86c6-4a38-8cac-5eab2cad271a/e-Conomy-Africa-2020-Exe-Summary.pdf?MOD=AJPERES&CVID=nmPYAEV.

18 African Development Bank Group, "Light Up and Power Africa: A New Deal on Energy in Africa," African Development Fund, accessed August 30, 2021, https://www.afdb.org/en/the-high-5/light-up-and-power-africa-%E2%80%93-a-new-deal-on-energy-for-africa#:~:text=Universal%20Access%20to%20Electricity&text=Over%20640%20million%20Africans%20have,the%20lowest%20in%20the%20world.&text=Similarly%2C%20the%20technical%20po

tential%20of,and%20geothermal%20energy%20is%20significant.

19 Statista, "Adult Literacy Rate in Africa as of 2019, by Region," May 5, 2021, https://www.statista.com/statistics/1233204/adult-literacy-rate-in-africa-by-region/.

20 Salah-Eddine Kandri, "Africa's Future is Bright—and Digital," World Bank Blogs, October 23, 2019, https://blogs.worldbank.org/digital-development/africas-future-bright-and-digital.

21 AfriLabs, A Resilient Africa 2020, https://www.afrilabs.com/wp-content/uploads/2020/04/2020_-A-Resilient-Africa.pdf.

22 Hamid Maher, Anas Laabi, Lisa Ivers and Guy Ngambeket, "Overcoming Africa's Tech Startup Obstacles," Boston Consulting Group, 2020, https://www.bcg.com/publications/2021/new-strategies-needed-to-help-tech-startups-in-africa.

23 Tage. Kene-Okafor, "How African Startups Raised Investments in 2020," Techcrunch, https://techcrunch.com/2021/02/11/how-african-startups-raised-investments-in-2020/.

24 Paula Gilbert, "Four Countries Take Lion's Share of Africa's Startup Funding," Connecting Africa, 2021, http://www.connectingafrica.com/author.asp?section_id=761&doc_id=766866.

25 Gilbert, "Four Countries."

26 Rogers, Diffusion of Innovation.

27 Zipporah Musau, "Africa Grapples with Huge Disparities in Education," Africa Renewal, December 2017–March 2018, https://www.un.org/africarenewal/magazine/december-2017-march-2018/africa-grapples-huge-disparities-education.

28 Organisation for Economic Co-operation and Development, Africa's Development Dynamics 2021: Digital Transformation for Quality Jobs (Paris: OECD, 2021), https://www.oecd.org/development/africa-s-development-dynamics-2021-0a5c9314-en.htm.

29 International Telecommunication Union, "ICT Development Index: A Proposal."

30 Global Commission on the Stability of Cyberspace, Advancing Cyberstability: Final Report (GCSC, November 2019), https://cyberstability.org/report/.

31 J. Kaplan, W. Richter, and D. Ware, Cybersecurity: Linchpin of the Digital Enterprise (McKinsey & Co., 2019), https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/Cybersecurity%20Linchpin%20of%20the%20digital%20enterprise/Cybersecurity-Linchpin-of-the-digital-enterprise.ashx.

32 Africanews, "Cyberattacks in Africa Comparable to Other Parts of the World, Says Kasperksy," July 2020, https://www.africanews.com/2021/07/20/cyberattacks-in-africa-comparable-to-other-parts-of-the-globe-says-kaspersky//.

33 Africanews, "Cyberattacks in Africa."

34 Serge Valery Zongo, "Establishment of CERTs/CIRTs in the Region," August 2018, https://www.itu.int/en/ITU-D/Capacity-Building/Documents/IG_workshop_August2018/Presentations/Session5_SergeZongorev.pdf.

35 International Telecommunication Union, Global Cybersecurity Index 2020 (Geneva: ITU Publications, 2021), https://www.itu.int/epublications/publication/global-cybersecurity-index-2020/en/.

36 African Union, The Digital Transformation Strategy for Africa (2020–2030), https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf.

37 Claudio Scardovi, Digital Transformation in Financial Services (Springer, 2017).

38 Narcisa Roxana Mosteanu, "Finance Digitalization and its Impact on the Labor Market," Technium Social Sciences Journal 8 (2020): 598–605.

About the Author

Bitange Ndemo is Professor of Entrepreneurship at the University of Nairobi's Business School. His research centers on the link between ICTs and small and medium enterprises with emphasis on how ICTs influence economic development in Africa. Prof. Ndemo Chairs the Kenya Distributed Ledgers and Artificial Intelligence Taskforce that developed the country's a road map for digital transformation. He is an advisor and Board member to several organizations, including Safaricom, one of the leading telecommunication company in Africa, a member of the OECD Expert Panel for Artificial Intelligence and Blockchain, and the World Economic Forum's Global Blockchain Council (part of the World Economic Forum's Global Fourth Industrial Revolution Councils). Besides having been a Permanent Secretary of Kenya's Ministry of Information and Communication, where he was credited with facilitating many transformative ICT projects, he is a Senior advisor to UN's Global Pulse (Big Data initiatives) and the UNCDF's Better than Cash Alliance and UNICEF's Innovation Council. He is an Open Data/Big Data evangelist and dedicated to simplification (visualization) of data for ordinary citizens to consume. He writes two columns every week for the Business Daily and Nation on-line.

Cyberstability Paper Series

New Conditions and Constellations in Cyber

Is There Space for a Digital Non-Aligned Movement?

Latha Reddy
Co-Chair of the Global Commission on the Stability of Cyberspace,
Former Deputy National Security Advisor of India

Anoushka Soni
National University of Juridical Sciences, Kolkata

Is There Space for a Digital Non-Aligned Movement?

Latha Reddy | Co-Chair of the Global Commission on the Stability of Cyberspace, Former Deputy National Security Advisor of India

Anoushka Soni | National University of Juridical Sciences, Kolkata

In an increasingly interconnected world, the discourse surrounding international norm settings in cyberspace has taken center stage. Digital rivalries between major world powers, particularly the United States and China, have necessitated a reevaluation of geopolitical affiliations by a number of historically neutral or non-aligned nations, such as India, Brazil, and others, when these countries take into consideration their national economic and security concerns. It is evident that, in this situation of increasingly great power polarity, many countries are seeking the creation of an alternative political space that allows them to exercise strategic autonomy. The formation of the Non-Aligned Movement in 1961 was a product of similar desires, and the same incentive now exists that demands a relook at traditional notions of non-alignment, as well as the emergence of new conceptualizations of non-alignment for a digital age.

Firstly, this paper addresses the increasingly heated debate on digital issues, and the various geopolitical, economic and security concerns that have arisen out of them, with a focus on 5G implementation as a case study. It also analyzes the traditionalist notion of the Non-Aligned Movement ("NAM")—its concerns, advocacy efforts, and the space it occupies within this digital age. Secondly, the paper engages with the notion of Europe as the new face of non-alignment, and details the

Latha Reddy is Co-Chair of the Global Commission on the Stability of Cyberspace. She is the former Deputy National Security Adviser of India, where she was responsible for cybersecurity and other critical internal and external security issues. Previously she also served as a Commissioner on the Global Commission on Internet Governance.

Anoushka Soni is a final year law student at the National University of Juridical Sciences, Kolkata. She has an avid interest in technology as well as international law, and was the Associate Director of the Society for International Law and Policy at NUJS.

individual and divergent concerns plaguing leading European nations. It also proposes a model for European integration on the 5G issue, through regional collaboration, flexibility, and identification of common ground. Finally, the paper attempts to bring together the traditional ideas of non-alignment with the emerging ones, and proposes a joint 5G Initiative requiring involvement of leaders in the European Union ("EU") as well as NAM, to usher in a new era of digital non-alignment.

The formation of the Non-Aligned Movement itself came from the desire to exercise greater collective bargaining power against existing "superpowers," while remaining detached from the conflict. The members of NAM concerned themselves with ensuring that they were not left as mere spectators in paramount issues of global importance, such as the nuclear arms race. They first came together to demand that a seat at the nuclear policy-making table could not be restricted solely to those states that were the reason for, or part of, the problem, and that being a potential victim of the use of nuclear weapons was a sufficient stake in the issue. Given that technology was a crucial factor in the clash between the United States and the Soviet Union during the first Cold War, it is unsurprising that the current conflict between the United States and China is being termed as the "next Cold War" and is similarly entrenched within emerging digital technology issues.[1]

A major issue of global concern that finds itself center stage at present is the deployment of fifth generation cellular networks, or 5G, and therefore is the primary focus of this analysis. Although the 5G debate may be seen as newly emerging, its foundations were laid down years ago, when, in 2012, the US House Intelligence Committee released an "Investigative Report on the US National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE."[2] The Investigative Report primarily raised concerns on the surveillance capabilities of these companies, and the national security threat to the US that letting them set up on American soil would pose. This escalated in 2020, when the Federal Communications Commission ("FCC") formally designated Huawei and ZTE as "national security threats" on account of accusations of their affiliations with the Chinese government, and of their harvesting data of US citizens.[3]

The strengths in Chinese 5G technology lie primarily in the higher quality and its lower cost as compared to the technology offered by its European competitors.[4] However, concerns over Chinese technology have never been about quality considerations, but rather suspicion over surveillance and security issues, and the increasing supremacy accorded to these concerns over economic considerations has led to a cascading effect across the world economy. This is only exacerbated through Chinese surveillance laws, which mandate cooperation with the government upon request,[5] as well as the existing affiliation that exists between large Chinese companies and the ruling Communist Party.[6] The blocking of Huawei and ZTE by the US have been accompanied by restrictions on chip-making equipment, leading to losses amounting to billions of dollars in profits for the semiconductor industry.[7] The consequences of these measures within the US are not restricted to monetary losses only, but go beyond them into constricting the amount the semiconductor companies can spend on research and development into improving their own technology.[8] Simultaneously, the Chinese semiconductor industry remains underdeveloped and reliant on foreign—mostly US—chip providers, or European manufacturers of semiconductor fabrication machinery, and therefore the ban had an impact on Chinese semiconduction production as well. Therefore, the trade war on semiconductors could lead to the unintended effect of a decline in the quality of cutting-edge technology within the US, while simultaneously hampering China from building expertise in specialist chips. The conflict will also manifest itself in developing nations, specifically those in Eastern Europe and Africa, where Chinese equipment, due to its substantially lower cost, forms the bulk of the basis of Internet access in the region.[9] While the US may be able to afford the economic consequences of banning Chinese companies, taking this hardline stance without

providing its developing friends and allies with an alternative may end with the world divided not only on political lines, but with a redrawing of those lines out of economic necessity, and with states prioritizing the responsibility they have to their own people.

The pervasive nature of this dispute cannot be constrained bilaterally to one between the US and China. It is part of a wider supply chain security issue, given the opposing interests and alliances at stake, and could lead to the burgeoning of a "Cold War 2.0," which is to be fought not on moralistic and ideological grounds, but instead on technological lines through trade battles and economic coercion.[10] Countries such as the United Kingdom ("UK"), which had initially allowed Huawei's participation in its 5G infrastructure, have reversed their decision on security grounds.[11] Countries in the Gulf, such as Saudi Arabia, Bahrain, and Qatar, etc.,[12] as well as Asian powers such as India,[13] have also been forced by their various specific geopolitical concerns, weighed against economic interests as well as foreign pressure, to enter into the 5G debate.

To mitigate the impact of this conflict, NAM must once again come together to ensure the free flow of technology and data, while simultaneously guaranteeing protection to the sovereign interests of nations. There must be an active attempt to achieve digital non-alignment, which requires economic investments and political strategy decisions to be made in such a way so as to avoid dependence on digital products from either the US or China.[14] The members of NAM are uniquely placed in this regard, since their individual geopolitical and economic considerations often compel them toward non-alignment as a political philosophy. To achieve their objectives, NAM has made submissions to various multilateral forums such as the Open-ended Working Group ("OEWG") as established by the UN General Assembly.

NAM must once again come together to ensure the free flow of technology and data, while simultaneously guaranteeing protection to the sovereign interests of nations.

The primary concerns on international cybersecurity iterated by NAM are first, that cyberspace will become a "theatre of military operations" through the development of cyber-offensive capabilities and the malicious use of ICTs, which will adversely impact the integrity and security of state infrastructure.[15] Second, there is the possibility of the adoption of unilateral measures beyond the ambit of the Charter of the United Nations and international law, which must be avoided so as not to impede the economic and social development of affected countries. Third, there is the concern that the development of an international legal framework would not be consensus-based but "top down" by a very small, self-appointed group, and therefore NAM has advocated for a framework within the UN with "active and equal" participation of all states. This must be accompanied by a multilateral inclusive institutional platform solely dedicated to international cooperation on safeguarding the peaceful uses of ICTs. Their final concern is that the digital divide between connected and less connected nations will continue to impact them adversely, leading to NAM recommendation that the digital divide be transformed into digital opportunities, for inclusive and non-discriminatory access to knowledge, and extension of support to developing countries in capacity building.

The final report by the OEWG addresses most of the concerns put forth by NAM, barring the recommendation that the legal framework must be accompanied by a "multilateral inclusive institutional platform dedicated to international cooperation on safeguarding the peaceful use of ICTs."[16] The NAM statement, though ambiguous, may be seen as seeking the establishment of a permanent forum within the UN, which is multilateral, inclusive and institutionally dedicated to international cooperation in ICTs. However, the OEWG report reiterates the OEWG itself as a "democratic, transparent, and inclusive platform" as well as the initiator of regular institutional dialogue on the

developments in ICTs in the context of international security. There exists a visible contrast between NAM's constant emphasis on multilateralism,[17] which is theoretically defined as the coordinated diplomatic interaction of three or more states in international politics, often accompanied by a commitment to certain core values,[18] and the OEWG's insistence on restricting "multilateral" only to the level of dialogue that must be achieved. Further, in a sphere where discourse is increasingly divided, the fear of resort to unilateralism and unilateral solutions is pervasive, and that is why NAM views multilateralism as the only sustainable method of addressing these security concerns.

The enhanced focus on the security implications of 5G, and the pervasive presence of national security concerns in 5G decisions taken by countries such as India, the UK, and the US, etc., evince that this issue has become entrenched within a sphere that has traditionally been governmental prerogative. National security issues are at the forefront of what states consider primarily governmental decisions, which may justify the necessarily multilateral leaning of the 5G debate in recent times. Effective multistakeholder involvement in 5G would, therefore, be limited to non-critical spheres such as infrastructure development and capacity building, and a governmental prioritization of national security concerns may overshadow these. Further, existing multilateral forums, such as the International Telecommunications Union ("ITU"), that are working on telecommunications and could contribute to the 5G debate by inclusion of their existing stakeholder groups, have so far directed their focus toward a technical analysis of the costs and vulnerabilities of the 5G network, rather than transforming themselves into a forum for engagement on the broader discourse around 5G.[19] This change of focus is perhaps linked to the existing ITU Secretary-General Zhao Houlin being a Chinese national, and China being the fifth-largest contributor to the ITU's budget as well, which has allowed it to play a central role in international standard setting.[20]

However, a leaning toward multilateralism need not mean the exclusion of the multistakeholder model, as evinced by the nonstate consultation process around the first UN OEWG,[21] or the accessibility of the Group of Governmental Experts on Lethal Autonomous Weapon Systems ("GGE LAWS") to non-state actor participation. The GGE LAWS, for instance, a primarily inter-governmental forum, contains representatives of non-governmental organizations, various law schools, universities, and research institutes who also actively participate and contribute, despite LAWS ostensibly being an issue of national security.[22] Therefore, the multilateral approach adopted by the GGE on LAWS is not independent of stakeholder input, to ensure transparency and accountability in the process. Similarly, primarily multistakeholder models, such as the Internet Governance Forum ("IGF"), have proposed extensions such as the IGF Plus, which is intended to provided additional multistakeholder and also multilateral legitimacy.[23] These proposals recognize the importance of multilateral input in addressing shortcomings of the multistakeholder model, such as lack of actionable outcomes due to limited government participation, especially from small and developing countries.

Simultaneously, while NAM members often attempt to maintain neutrality to access these multistakeholder frameworks, they are compelled by their own competing economic and security interests to take a stance on such issues. For instance, the Indian position on 5G was reflective of a desire to balance these interests, which devolved into an increasingly clear exclusion of China from the Indian market. Though India initially permitted all applicants to participate in 5G trials,[24] a security review was later mandated with an emphasis on Chinese companies specifically,[25] and the border skirmish in the Galwan valley led to a ban on 260 Chinese smart phone apps on national security grounds.[26] Subsequently, the Department of Telecommunications of India permitted the conduction of trials for the usage and application of 5G technology by telecom service providers, including Ericsson, Nokia, Samsung, and C-DOT, with a notable absence of Chinese equipment

manufacturers.[27] India's position, with it being a founding and influential member of NAM, may influence other members of NAM to clarify their strategic orientations, and to abandon neutrality in favor of crucial national interests.

In other spheres of international debate where NAM has exercised influence, their statements carry weight because the interests of all their members align, such as in the case of LAWS under the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects ("CCW"). The statement made by NAM before the GGE concretely calls for a legally binding international instrument that has provisions both for the prohibition and regulation of LAWS.[28] Through extensive lobbying, especially with states that are concerned about the increasingly asymmetric nature of warfare and reflecting such concerns in their statements, NAM was able to achieve consensus building on a polarized issue, and exert their influence on a global stage. In the case of LAWS, members of NAM are similarly situated, since most developing nations have not achieved the technological advancement necessary to develop their own fully autonomous weapons systems. However, unlike LAWS, the individualistic national security nature of the 5G debate presents a diverging set of state-specific issues when compared to the global ethical and security concerns of asymmetric warfare that LAWS raises.[29] Therefore, similar consensus building across all emerging technologies will mean achieving the unlikely goal of setting aside these individual security concerns in favor of collective interests.

With the positions of the members of NAM and their alliances in the Digital Cold War remaining uncertain, it remains to be seen whether Europe can provide a middle ground among the technological protectionism and trade clashes escalating globally. The absence of a unified position within Europe on the 5G issue is indicative of a larger divide in the European system itself. The 5G debate was most politicized within the United Kingdom, where access was initially granted to Huawei; however, following the sanctions imposed on Huawei by Washington, UK mobile providers were subsequently, first, banned from buying new Huawei 5G equipment and, second, mandated to remove any existing equipment by 2027.[30] The economic infeasibility of such decisions is highlighted by the UK Digital Secretary, who estimated the cost of this move to be two billion pounds, coupled with two to three years of delay in the 5G rollout.[31]

It remains to be seen whether Europe can provide a middle ground among the technological protectionism and trade clashes escalating globally.

The UK is one of the staunchest allies of the United States, and therefore, the political necessity demanding the UK's position in this conflict is understandable. However, Germany, another US ally, has also been internally divided on the 5G issue, taking a position of "strategic equidistance," which is reflected both in its legal and policy approaches to the 5G issue; not wishing to impact mutually beneficial trade relations with China. For instance, on the legal front, Germany's new amendments to the Information Technology Security Act contain what is popularly known as the "Huawei clause,"[32] which, interestingly, provides for a two-part assessment mechanism, consisting of a technical evaluation accompanied by a declaration that the components purchased cannot be used for sabotage or espionage.[33] While ostensibly a neutral measure, the law is qualified by the requirement that vendor safety provisions, through the exclusion of vendors, are only triggered if all authorities involved unanimously wish to ban a vendor, which, given the wide ranging and controversial nature of this debate, is an unlikely occurrence. Accompanied by a lack of specific exclusion of any one vendor, notably Huawei, the increased legal hurdles in banning vendors are an attempt to walk a fine line between pressure from the US and the protection of its own economic interests.[34]

Germany's position on 5G and the primacy it accorded to economic considerations over external pressure is likely to be followed by other members of the EU, and similar measures were adopted by France and Italy, while softer stances were taken by Hungary, Spain, and Slovakia, etc.[35] The Italian government, similar to the German approach, has retained the power to veto any deals for the supply of 5G which it views as a threat to its national security. This power has, in fact, been exercised in the case of Huawei, where their deal with Fastweb was prohibited due to the processing of highly sensitive data involved. However, Vodafone (UK) recently secured approval to use Huawei equipment, illustrating that there is no clear targeting of Chinese manufacturers under the law.[36] France has taken another divergent approach, by adopting a phase-out process, and prohibiting renewal of licenses for Huawei equipment—thereby ensuring that within three to eight years the country is not reliant on the same.[37]

Hungary however, remains open to cooperating with China on economic and technological issues, and Huawei has been allowed to open a new research and development center in Budapest, which is largely seen as favoring Hungary's strategic and economic interests.[38] Further, barring restrictions at the broader, multilateral level of the EU, Hungary has no incentive to incur the kind of costs that removal of Chinese companies from within its economy would require, when they have already begun working together in key areas such as public institutions, emergency services, educational and health institutions, and public, state-owned companies.[39] Similarly, Spain has adopted a "neutral and independent" approach, refusing to de facto ban any supplier outright, and instead adopting a risk assessment mechanism to allow or ban mobile companies from partaking in the 5G rollout.[40] Poland and Romania have further signed bilateral deals with the United States to permit only "trusted" suppliers of 5G networks, a move that has been challenged by Huawei as violative of EU law.[41]

The varying political, security, and economic considerations that accompany the 5G debate have led to an absence of an extreme stance, notably a ban, being taken by Brussels. The report issued by the EU on coordinated risk assessment on cybersecurity in 5G networks identifies a key risk in the implementation of 5G as an increased and major dependance on a single supplier, which could lead to supply interruptions.[42] Further, the report identifies that dependence on suppliers presenting a "high degree of risk" increases the impact of vulnerabilities and their exploitation by third party malicious actors. EU as a whole seems to be adopting a flexible approach, allowing its members to determine what part Chinese companies can play in their 5G networks.[43] The EU endorses individual risk assessment mechanisms, which demand evaluation of vendors on technical competency as well as national security concerns. The potential for consensus building lies in flexibility, as well as in risk assessments which could also include mandatory signing of "no-spy" agreements with high-risk vendors, such as the one Huawei was willing to sign with governments including the UK.[44] The EU is considering a collective risk assessment model, whereby vendors would be declared as high risk at a regional level, and would be subject to security enhancement obligations, allowing the EU to achieve their objective of cooperation on cybersecurity.[45] Further, since the primary competitors to Chinese 5G developers are companies founded within Europe, such as Vodafone, Ericsson, and Nokia, etc., a regional funding model to provide alternatives to Chinese equipment may be considered.[46] These proposed alternatives could form an integral part of European digital policy to ensure that technological sovereignty, which is European autonomy in the digital sector, is a realizable aim.

Traditionally, the European governance model focuses on establishment of multistakeholder efforts,[47] giving non-state actors authority in policy processes at a global scale. However, consensus building surrounding 5G and other cybersecurity issues requires a renewed focus into multilateral

ism to ensure broader global cooperation. The EU has adopted the multistakeholder model in their other region-wide initiatives, such as the General Data Protection Regulation ("GDPR"), where the European Commission, an inter-governmental body, established a multistakeholder expert group under its aegis to assist the identification of challenges in GDPR application from different stakeholder perspectives.[48] The European experience during and after both World Wars necessitated protection for privacy and personal information, which then evolved into fundamental rights in the EU.[49] In the US, however, privacy rights are balanced with commercial interests of other entities, and data privacy occasionally finds itself fundamentally opposed to the absolutist protection given to free speech within the US.[50] China has taken a third approach to data protection through a patchwork of legal instruments and non-binding rules, which has brought it closer to global standards.[51] In the sphere of data protection, the GDPR stands out as the instrument that places privacy at its forefront, not only within the EU, but it also requires data transfers from countries outside the EU to comply with these stringent norms. While concerns have been raised over the economic feasibility of these for smaller businesses, the EU has largely emerged as an alternative to the minimalist and state-centered data protection models of US and China, to set its own global standards. The level of protection under the GDPR was upheld only through the creation of various bilateral and plurilateral instruments mandating GDPR or other similar protection as the minimum standard. Therefore, while multistakeholderism played a crucial role in the conceptualization and implementation of the GDPR at an EU-wide level, multilateralism helped translate the GDPR into the global baseline for data protection. As a result, through increased cooperation at the regional level, continuous dialogue and knowledge sharing, Europe could be uniquely placed to lead the way in consensus building at a global level—its desire for strategic autonomy and appreciation of European interests giving it a central NAM-like role.[52]

A review of the position taken by NAM, along with the comprehensive analysis on the European dilemma, raises the question of a potential alliance for the future of digital non-alignment. The conceptualization of non-alignment has historically been linked to neutrality. However, neutrality is not a static concept, and the ability of a state to remain neutral depends on each state's prevailing individual political, geostrategic, economic, and social conditions. The primacy given to ideology during the first Cold War no longer exists today, and countries prefer to prioritize their economic and security interests. Viewing technological issues through political lenses, such as is being done by the US in their outright ban on Chinese equipment, is a myopic vision that the US expects its allies to unconditionally adopt. Unsurprisingly, countries in the EU and within NAM do not see this issue in such distinct black and white terms, and wish to segregate their economic dealings with China from their political ramifications.

The 5G debate is only the beginning of a world divided along technological lines, with the US and China primarily facilitating this divide.

The 5G debate is only the beginning of a world divided along technological lines, with the US and China primarily facilitating this divide. The digital era brings with it new challenges and concerns that plague countries today, and, in a digitally globalized world, the solutions to these problems necessitate global cooperation. Some of the key considerations that the UN Roadmap for Digital Cooperation highlights are the requirement for an inclusive digital economy and society, human and institutional capacity building, digital human rights, digital trust and security, and global digital cooperation.[53] An absence of one of the above may impact the others, such as in the 5G debate, where the absence of digital trust and security due to use of what is perceived to be potentially malicious technology, directly and adversely hinders global digital cooperation in other areas.

The solutions to these concerns highlighted by the UN Roadmap require global cooperation initiatives, bringing together diverse approaches to governance frameworks, thereby incorporating both NAM's focus on multilateralism, and the EU focus on multistakeholderism, to create platforms such as a joint EU-NAM 5G Initiative. 5G is an issue in which EU and NAM are uniquely placed, with their economic considerations requiring the creation of a non-aligned alternative to the US-China binary. The joint 5G Initiative could pave the way for EU-NAM cooperation on other digital issues of global concern, especially where there exists a similar convergence of positions due to prioritization of economic concerns, absence of existing, sufficiently competitive alternatives for self-reliance, and a desire to exercise collective influence to de-escalate global repercussions of trade conflicts. There will necessarily exist areas within cybersecurity where such cooperation may be unable to be achieved, such as data protection, where Europe's advanced technological infrastructure, coupled with regional cultural influences, allows it to place privacy on the highest pedestal—something which the primarily developing countries that compose NAM are unable to do.[54] However, the proposed initiative remains crucial for opening a dialogue of digital cooperation focused on non-alignment between two regional groups that have not exercised formal opportunities for collaboration in the past. It could also be a steppingstone to the creation of a multilateral inclusive institutional platform as NAM has called for,[55] with a more even distribution of power within it. Such an initiative could be set up jointly by NAM and the EU, with one influential country from each grouping being given joint leadership. For instance, an EU-NAM initiative led by Germany and India would ensure that countries that are seen as key players within their respective regions are provided a platform to lead collaboration on a global scale. Given that the India–EU summit has already begun discussions on collaboration in the field of 5G,[56] and India's upcoming presidency of the G20,[57] India's leadership role here will facilitate coordination not only with NAM but also with the EU. This initiative must be subsequently promoted and encouraged at meetings within the EU, as well as at preparatory and official summit meetings of the NAM Contact Group. After achieving sufficient interest generation, preparatory dialogue for various administrative aspects of the Initiative may begin, which would include discussions on the Secretariat, funding, and cooperative frameworks, etc.

The crux of the initiative should be its approach toward 5G technologies—especially given the divergent positions of various states that would be party to this initiative. Most developing countries within the 5G debate are primarily concerned with avoiding technological asymmetry and do not wish to be left behind in the 5G race, nor deprived of its infrastructural benefits that would improve crucial areas such as health, education, and defense, etc.[58] However, these desires are sometimes overshadowed by the national security concerns at stake, which have been at the heart of the debate surrounding 5G. Therefore, the initiative must adopt a flexible yet cohesive framework, taking inspiration from initiatives for regional cooperation adopted within the EU. Ideas such as collective risk assessment models, flexibility—with a margin of appreciation given to each member state to the extent to which high risk vendors shall be used, subject to certain additional safeguards such as "no-spy" agreements, entity-level identification of high-risk vendors, an emphasis on the phasing out of high-risk vendors by 2030, etc., would ensure that there is a degree of interoperability achieved within the initiative while still accounting for individualistic national concerns.

Simultaneously, while high-risk vendors, traditionally considered to be Huawei and ZTE due to pervasive domestic law requirements in China,[59] are being phased out of the backbone of national networks, alternatives to these high-quality and low-cost technologies must also be considered to ensure that developing countries are not left without access to 5G. The funding model adopted by the EU-NAM initiative could be used to create a 5G Implementation Initiative under the aegis of the broader initiative, where regional players from the EU and NAM member states can come to

gether to collectively develop alternatives to Chinese technologies. These would require existing market players within the EU to collaborate with companies working on 5G within other states who are party to the initiative to collaboratively develop these viable and cost-effective alternatives. The initiative must ensure that it creates space for those countries that wish to rely on Chinese 5G technology, through imposing greater compliance obligations, while also providing alternatives to other countries moving away from Chinese technology on security grounds.

The Initiative may also lead the way in ensuring global adoption of proposals such as a Digital Stability Board, modeled around the Financial Stability Board, which could play a crucial role in regulation, best practices, and standard setting.[60] The Digital Stability Board, as visualized by the Centre for International Governance Innovation, is seen as an intergovernmental body, working with various stakeholders on the coordination and development of standards on an inclusive list of digital concerns.[61] The current centrality of 5G implies that the Board could play a role in norm setting in the sphere, and also pave the way for the development of norms around 6G. Since one of the proposals in this regard is for the Board to oversee personal information as data trusts,[62] which is being incorporated into the domestic law of countries such as India,[63] the Initiative would be uniquely placed to craft multilateral consensus on this. Given China's large investments in Europe, and its efforts toward European partnerships,[64] the Initiative could also pave the way for a multilateral dialogue with China. This would allow the initiative to truly achieve non-alignment in the digital sphere.

The Initiative may also lead the way in ensuring global adoption of proposals such as a Digital Stability Board, modeled around the Financial Stability Board, which could play a crucial role in regulation, best practices, and standard setting.

Despite evident ideological and political divides between certain members of the EU and NAM, including on issues that form a core part of digital cooperation, they are at least temporarily bound by the mutual desire to remain independent in a primarily bilateral conflict, with the world caught in its crosshairs. Therefore, a digital future led jointly and equally by the EU and NAM through this initiative could provide an attractive model of non-alignment for a large number of countries in Africa, Asia, and South America, who find themselves torn between either end of this debate, and assist them in achieving a balance in an increasingly polarized world. Digital non-alignment must be secured by leaders of the EU and NAM, since the fate of the digital era and the de-escalation of a Digital Cold War rests on this unlikely, yet mutually beneficial, potential alliance for the future.

Endnotes

1 Yang Yao, "The New Cold War: America's new approach to Sino-American relations," China International Strategy Review 3, 20–33 (2021), https://link.springer.com/article/10.1007/s42533-021-00071-1; Dealbook, "Inside the New Tech Cold War," October 1, 2020, https://www.nytimes.com/2020/10/01/business/dealbook/tech-cold-war-us-china.html.

2 Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE, H.R. Rep. (2012)

3 Aashish Aryan, "US says Huawei, ZTE are 'national security threats': How will this impact India?," The Indian Express, July 1, 2020, https://indianexpress.com/article/explained/us-fcc-huawei-zte-national-security-threats-6484631/.

4 Robert Clark, "China aims to drive down 5G power cost," Light Reading, March 11, 2020, https://www.lightreading.com/asia/china-aims-to-drive-down-5g-power-cost/d/d-id/765140; Chen Qingqing and Shen Weiduo, "Political factors aside, Ericsson can't compete with Huawei: analysts," Global Times, May 12, 2021, https://www.globaltimes.cn/page/202105/1223316.shtml.

5 Robin Emmott, "China's intelligence law looms over EU 5G safeguards: official," Reuters, July 19, 2019, https://www.reuters.com/article/us-eu-huawei-tech-idUSKCN1UE18I.

6 Gautam Chikermane, "No Huawei in 5G is a start, No China in critical infrastructure should be next," Observer Research Foundation, May 5, 2021, https://www.orfonline.org/expert-speak/no-huawei-in-5g-is-a-start-no-china-in-critical-infrastructure-should-be-next/.

7 Stu Woo, "The US vs China: The high cost of the technology cold war," Mint, October 23, 2020, https://www.livemint.com/news/world/the-us-vs-china-the-high-cost-of-the-technology-cold-war-11603441980369.html.

8 Chad P. Bown, "How Trump's export curbs on semiconductors and equipment hurt the US technology sector," Peterson Institute for International Economics, September 28, 2020, https://www.piie.com/blogs/trade-and-investment-policy-watch/how-trumps-export-curbs-semiconductors-and-equipment-hurt-us.

9 Stu Woo, "The U.S. vs. China: The High Cost of the Technology Cold War," The Wall Street Journal, October 22, 2020, https://www.wsj.com/articles/the-u-s-vs-china-the-high-cost-of-the-technology-cold-war-11603397438.

10 Marc Champion, "How U.S.-China Tech Rivalry Looks Like a Digital Cold War," Bloomberg, December 12, 2019, https://www.bloomberg.com/quicktake/how-u-s-china-tech-rivalry-looks-like-a-digital-cold-war; Enda Curran, "Paulson Warns of 'Economic Iron Curtain' Between US, China," Bloomberg, November 6, 2018, https://www.bloomberg.com/news/articles/2018-11-07/paulson-warns-of-economic-iron-curtain-between-u-s-china.

11 Bloomberg, "UK told Huawei that US pressure contributed to ban: Observer," The Indian Express, July 19, 2020, https://indianexpress.com/article/technology/tech-news-technology/uk-government-us-pressure-huawei-ban-5g-observer-6513037/; Jonathan Shieber, "UK government reverses course on Huawei's involvement in 5G networks," May 24, 2020, https://techcrunch.com/2020/05/23/uk-government-reverses-course-on-huaweis-involvement-in-5g-networks/.

12 Mohammed Soliman, "The GCC, US-China tech war, and the next 5G storm," Middle East Institute, September 1, 2020, https://www.mei.edu/publications/gcc-us-china-tech-war-and-next-5g-storm.

13 Harsh V. Pant and Aarshi Tirkey, "India Draws a Line in the 5G Sand," Observer Research Foundation, May 19, 2021, https://www.orfonline.org/research/india-draws-a-line-in-the-5g-sand/.

14 Parminder Jeet Singh, "India should aim for a digital non-alignment," Hindustan Times, July 2, 2019, https://www.hindustantimes.com/analysis/india-should-aim-for-a-digital-non-align

ment/story-ViT3PTiuo5j6dKUvt94YpO.html.

15 NAM Statement, "OEWG on developments in the field of information and telecommunications in the context of international security," Informal Virtual Meeting, February 18–22, 2021, https://front.un-arm.org/wp-content/uploads/2021/02/NAM-Statement-Informal-Consultation-OEWG-on-ICT.pdf.

16 UN General Assembly, Open-ended working group on developments in the field of information and telecommunications in the context of international security, Final Substantive Report, A/AC.290/2021/CRP.2, (March 10, 2021), https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

17 NAM Working Paper for the Second Substantive Session of the Open-ended Working Group on developments in the Field of Information and Telecommunications in the Context of International Security (OEWG), Remarks on the Pre-Draft Circulated by the OEWG Chair, https://front.un-arm.org/wp-content/uploads/2020/04/nam-wp-to-the-oewg-final.pdf.

18 Hanns W. Maull, "Multilateralism: Variants, Potential, Constraints and Conditions for Success," Stiftung Wissenschaft and Politik, March, 2020, https://www.swp-berlin.org/publications/products/comments/2020C09_multilateralism.pdf.

19 "5G—Fifth generation of mobile technologies," International Telecommunications Union, December 2019, https://www.itu.int/en/mediacentre/backgrounders/Pages/5G-fifth-generation-of-mobile-technologies.aspx.

20 Hideaki Ryugen and Hiroyuki Akiyama, "China leads the way on global standards for 5G and beyond," Financial Times, August 5, 2020, https://www.ft.com/content/858d81bd-c42c-404d-b30d-0be32a097f1c.

21 "Outcome Report of the Informal Multistakeholder Consultation on OEWG Zero Draft Report," February 25, 2021, https://front.un-arm.org/wp-content/uploads/2021/03/Outcome-Report-of-the-Informal-Multistakeholder-Consultation-on-OEWG-zero-draft.pdf; "Open-ended Working Group," United Nations Office for Disarmament Affairs, https://www.un.org/disarmament/open-ended-working-group/.

22 Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons System, "Report of the 2019 session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapon System," CCW/GGE.1/2019/3, (September 25, 2019), https://documents.unoda.org/wp-content/uploads/2020/09/CCW_GGE.1_2019_3_E.pdf.

23 "Report of the UN Secretary General's High-level Panel on Digital Cooperation," Internet Governance Forum, https://www.intgovforum.org/multilingual/content/report-of-the-un-secretary-general%E2%80%99s-%E2%80%8Ehigh-level-panel-on-digital-cooperation.

24 Ministry of Communications, "Telecom Department gives go-ahead for 5G Technology and Spectrum Trials," news release, May 4, 2021, https://www.pib.gov.in/PressReleasePage.aspx?PRID=1715927.

25 Ministry of Communications, "5G field trials," news release, June 26, 2019, http://loksabhaph.nic.in/Questions/QResult15.aspx?qref=628&lsno=17.

26 India TV Tech Desk, "Complete list of 267 Chinese apps banned in India: PUBG Mobile, TikTok, AliExpress and more," India TV, November 24, 2020, https://www.indiatvnews.com/technology/news-list-of-all-chinese-apps-banned-in-india-2020-667131.

27 Lalit K Jha, "India's decision to allow 5G trials without Chinese companies is sovereign: US," Mint, May 12, 2021, https://www.livemint.com/news/india/indias-decision-to-allow-5g-trials-without-chinese-companies-is-sovereign-us-11620776922441.html.

28 Government of Venezuela, "General Principles on Lethal Autonomous Weapons Systems," Working Paper submitted on behalf of the Non-Aligned Movement (NAM) and other states parties to the Convention on Conventional Weapons Group of Governmental Experts on lethal

autonomous weapons systems, March 28, 2018, https://www.unog.ch/80256EDD006B8954/(httpAssets)/E9BBB3F7ACBE8790C125825F004AA329/$file/CCW_GGE_1_2018_WP.1.pdf.

29 "Autonomous Weapon Systems: Technical, Military, Legal and Humanitarian Aspects," International Committee of the Red Cross, November 2014, https://www.icrc.org/en/document/report-icrc-meeting-autonomous-weapon-systems-26-28-march-2014.

30 Leo Kelion, "Huawei 5G kit must be removed from UK by 2027," BBC News, July 14, 2020, https://www.bbc.com/news/technology-53403793.

31 Annabelle Timsit, "The UK will ban Huawei from its 5G network earlier than expected," Quartz, November 27, 2020, https://qz.com/1938635/uk-huawei-ban-could-be-implemented-earlier-than-planned/.

32 Stefan Krempl, "IT Security Act 2.0: "Middle finger in the face of civil society"," heise online, October 12, 2020, https://www.heise.de/news/IT-Sicherheitsgesetz-2-0-Mittelfinger-ins-Gesicht-der-Zivilgesellschaft-4986032.html.

33 Beryl Thomas, "What Germany's new cyber security law means for Huawei, Europe, and NATO," European Council on Foreign Relations, February 5, 2021, https://ecfr.eu/article/what-germanys-new-cyber-security-law-means-for-huawei-europe-and-nato/.

34 Matthew Karnitschnig, "How Germany opened the door to China – and threw away the key," Politico, September 10, 2020, https://www.politico.eu/article/germany-china-economy-business-technology-industry-trade-security/.

35 Yang Kunyi, "Slovakia believes Huawei can demonstrate transparency: Deputy prime minister," Global Times, November 12, 2019, https://www.globaltimes.cn/content/1169827.shtml.

36 Elvira Pollina and Giuseppe Fonte, "Italy gives Vodafone 5G deal with Huawei conditional approval – sources," Reuters, May 31, 2020, https://www.reuters.com/technology/italy-gives-vodafone-5g-deal-with-huawei-conditional-approval-sources-2021-05-31/.

37 Mathieu Rosemain and Gwénaëlle Barzic, "Exclusive: French limits on Huawei 5G equipment amount to de facto ban by 2028," Reuters, July 22, 2020, https://www.reuters.com/article/us-france-huawei-5g-security-exclusive-idUSKCN24N26R.

38 Pawel Paszak, "Huawei in Poland and Hungary. Could it be a part of 5G?," Warsaw Institute, November 30, 2020, https://warsawinstitute.org/huawei-poland-hungary-part-5g/.

39 Reuters Staff, "Hungarian minister opens door to Huawei for 5G network rollout," Reuters, November 5, 2019, https://www.reuters.com/article/us-hungary-telecoms-huawei-idUSKBN1XF12U.

40 Fernando Heller, "Spanish government to prepare a list of 'safe' 5G mobile providers," Euractiv, December 16, 2020, https://www.euractiv.com/section/5g/news/spanish-government-to-prepare-a-list-of-safe-5g-mobile-providers/.

41 Laurens Cerulus, "Huawei challenges legality of 5G bans in Poland, Romania," Politico, November 2, 2020, https://www.politico.eu/article/huawei-hints-at-legal-action-against-5g-bans-in-poland-romania/.

42 EU coordinated risk assessment of the cybersecurity of 5G networks, October 9, 2019, (NIS Cooperation Group); European Commission and the Finnish Presidency of the Council of the EU, "Member States publish a report on EU coordinated risk assessment of 5G networks security," press release, October 9, 2019, https://ec.europa.eu/commission/presscorner/detail/en/ip_19_6049.

43 Douglas Busvine, "Europe telecoms lobby group 'denounces' bans on Chinese vendors," Reuters, October 16, 2020, https://www.reuters.com/article/us-huawei-europe/europe-telecoms-lobby-group-denounces-bans-on-chinese-vendors-idUSKBN2711I7.

44 Paul Sandle, "Huawei willing to sign 'no-spy' pacts with governments: chairman," Reuters, May 14, 2019, https://www.reuters.com/article/us-huawei-security-britain-chairman/huawei-willing-to-sign-no-spy-agreements-with-governments-chairman-idUSKCN1SK1HL.

45 European Commission, "New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient," Press Release, December 16, 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391.

46 European 5G Observatory, "Recovery and Resilience Facility (RRF): 130 billion EUR," https://5gobservatory.eu/public-initiatives/public-funding-of-5g-deployment/.

47 "Joint comments from the EU and its Member States on the initial 'pre-draft' report of the Open-Ended Working Group on developments in the field of Information and Telecommunication in the context of international security," https://ceipfiles.s3.amazonaws.com/pdf/CyberNorms/UNGGE/Joint+Comments+from+the+EU+and+its+Member+States+on+the+Initial+%E2%80%98Pre-Draft%E2%80%99+Report+of+the+Open-Ended+Working+Group+on+Developments+in+the+Field+of+Information+and+Telecommunications+in+the+Context+of+International+Security.pdf.

48 Register of Commission Expert Groups and Other Similar Entities, "Multistakeholder expert group to support the application of Regulation (EU) 2016/679 (E03537)," 2017, https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?do=groupDetail.groupDetail&groupID=3537.

49 Charter of Fundamental Rights of the European Union, Dec.7, 2000, 2012/C 326/02, Art. 8.

50 U.S. Const. amend. I; Stephen Cobb, "Data privacy and data protection: US law and legislation," ESET White Paper, April 2016, https://www.researchgate.net/publication/309456653_Data_privacy_and_data_protection_US_law_and_legislation.

51 Emmanuel Pernot-Leplay, "China's Approach on Data Privacy Law: A Third Way Between the U.S. and the EU?", Penn State Journal of Law & International Affairs, 8, No. 1, (March 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3542820&__cf_chl_captcha_tk__=pmd_JcuRohxlGPngli9RYNCUw_Xd2GOGz7.wJUdDfKryp7c-1630170613-0-gqNtZGzNAuWjcnBszQw9.

52 Amandeep Gill, "Europe is the new NAM," Observer Research Foundation, January 16, 2021, https://www.orfonline.org/expert-speak/europe-is-the-new-nam/.

53 United Nations, Report of the Secretary General: Roadmap for Digital Cooperation, June 2020 https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf.

54 Bhaskar Chakravorti, "Why the Rest of the World Can't Free Ride on Europe's GDPR Rules," Harvard Business Review, April 30, 2018, https://hbr.org/2018/04/why-the-rest-of-world-cant-free-ride-on-europes-gdpr-rules; Prashant Reddy T., "Should There be a 'Developing Country' Template For Data Protection Legislation?," The Wire, May 17, 2018, https://thewire.in/tech/should-there-be-a-developing-country-template-for-data-protection-legislation; Rahul Matthan, "India need not adopt the onerous European General Data Protection Regulation," Mint, April 4, 2018, https://www.livemint.com/Opinion/xBXHfSpoq4sc71YH3XbsdL/India-need-not-adopt-the-onerous-European-GDPR.html.

55 NAM Statement, "OEWG on developments in the field of information and telecommunications in the context of international security," Informal Virtual Meeting, February 18–22, 2021, https://front.un-arm.org/wp-content/uploads/2021/02/NAM-Statement-Informal-Consultation-OEWG-on-ICT.pdf.

56 Archana Chaudhary, "EU official looks to align with India to protect democracy," Economic Times, April 19, 2021, https://economictimes.indiatimes.com/industry/telecom/telecom-news/eu-official-looks-to-align-with-india-on-5g-to-protect-democracy/articleshow/82145426.cms?-from=mdr.

57 Mohit Chowdhry, "A digital agenda for India's G20 presidency," Observer Research Foundation, June 1, 2020, https://www.orfonline.org/expert-speak/a-digital-agenda-for-indi-

as-g20-presidency/.

58 Kadri Kaska, Henrik Backvard and Tomáš Minárik, "Huawei, 5G and China as a Security Threat," NATO Cooperative Cyber Defence Centre of Excellence, 2019, https://ccdcoe.org/uploads/2019/03/CCDCOE-Huawei-2019-03-28-FINAL.pdf.

59 Samuel Stolton, "Huawei admit Chinese law obliges companies to work with government, under conditions," Euractiv, April 11, 2019, https://www.euractiv.com/section/cybersecurity/news/huawei-admit-chinese-law-obliges-companies-to-work-with-government/.

60 Rohinton P. Medhore, "A Post-COVID-19 Digital Bretton Woods," Centre for International Governance Innovation, April 19, 2020, https://www.cigionline.org/articles/post-covid-19-digital-bretton-woods/.

61 Robert Fay, "Digital Platforms Require a Global Governance Framework," Centre for International Governance Innovation, October 28, 2019, https://www.cigionline.org/articles/digital-platforms-require-global-governance-framework/; Daniel Garcia-Macia and Rishi Goyal, "Decoupling in the Digital Era," International Monetary Fund, 2021, https://www.imf.org/external/pubs/ft/fandd/2021/03/international-cooperation-and-the-digital-economy-garcia.htm.

62 Rohinton P Medhora, "We need a new era of international data diplomacy," Financial Times, January 18, 2021, https://www.ft.com/content/66f1ff42-fe49-4376-aafb-3943a9f-04a1c?shareType=nongift.

63 Trishi Jindal and Aniruddh Nigam, "Data Stewardship for Non-Personal Data in India," Vidhi Centre for Legal Policy, November 20, 2020, https://vidhilegalpolicy.in/research/data-stewardship-for-non-personal-data-in-india/.

64 Isabel Gacho Carmona, "The European Union before China's rise as a tech power: the 5G case," Instituto Espanol de Estudios Estrategicos, March 19, 2020, http://www.ieee.es/Galerias/fichero/docs_opinion/2020/DIEEEO23_2020ISAGAC_5G-ENG.pdf.

About the Authors

Latha Reddy is Co-Chair of the Global Commission on the Stability of Cyberspace. She served in the Indian Foreign Service from 1975-2011 and was appointed as India's Deputy National Security Adviser from 2011-2013 where she was responsible for cybersecurity and other critical internal and external security issues. She has extensive experience in foreign policy, and in bilateral, regional and multilateral negotiations. In addition, she has expertise on security and strategic issues and has worked on strategic technology policies, particularly on cyber issues relating to cyber security policy, international cyber cooperation and Internet governance. She served as a Commissioner on the Global Commission on Internet Governance and is involved with several organizations and think-tanks, both globally and in India. She is currently, among other positions, serving as a Distinguished Fellow in the EastWest Institute in the US and the Observer Research Foundation in India.

Anoushka Soni is a final year law student at the National University of Juridical Sciences, Kolkata. Anoushka has an avid interest in technology as well as international law, having been the Associate Director of the Society for International Law and Policy at NUJS. She has previously authored papers on Autonomous Weapon Systems at the Centre for Internet and Society, Bangalore and has additionally collaborated with the Association for Progressive Communications on their Internet Rules: Unboxing Digital Laws in South Asia workshop in 2020, as well as their Advocacy International: Advancing the Digital Rights Agenda for Asia, in 2021. Anoushka shall be joining a premier Indian law firm, Cyril Amarchand Mangaldas in their technology, media and telecommunications practice in 2022.

Cyberstability Paper Series

New Conditions and Constellations in Cyber

Closing the Gap: Expanding Cyber Deterrence

Michael Daniel
CEO of the Cyber Threat Alliance; Former Cybersecurity Coordinator, US National Security Council

Closing the Gap: Expanding Cyber Deterrence

Michael Daniel | CEO of the Cyber Threat Alliance; Former Cybersecurity Coordinator, US National Security Council

While cyber deterrence is a logical goal, it often seems rather elusive. Certainly, the volume, intensity, and impact of malicious cyber activity have grown substantially over the last few years, leading some thinkers and practitioners to argue that deterrence will not work in cyberspace. The public evidence points in the other direction, however: deterrence can and does work in cyberspace. Nation-states could undertake regular, sustained, destructive actions in and through cyberspace if they wished, but they do not, because deterrence affects their decision calculus. Instead of not functioning at all, cyber deterrence is insufficient in its current form.

First, a gap exists between activities that cannot be realistically deterred (such as espionage) and those that are already deterred (such as nation-states undertaking widespread, frequent, destructive cyberattacks against critical infrastructure assets outside of armed conflict). Yet, activity that falls within this gap causes measurable harm, violates internationally agreed upon norms or "rules of the road" of cyber behavior, and is potentially destabilizing to international peace. Second, malicious cyber activity is often cumulative in its effects, yet individually not all that harmful. Any single theft of intellectual property or business disruption might not rise to the level of a national security threat, but, taken collectively, these activities become significant problems. As a result, cumulative, counter-normative, and consistent malicious cyber activity falling within the deterrence gap threatens many nations, damaging their national security, reducing economic prosperity, and harming public health and safety. Given the physical characteristics of cyberspace and the multiplicity of malicious actors with different motivations, a single policy approach, such as Mutually Assured Destruction, cannot shrink this deterrence gap, nor can it reduce the volume, intensity, and impact of malicious activity that might occur in a smaller gap. Rather, expanding cyber deterrence requires

Michael Daniel is the President and CEO of the Cyber Threat Alliance. From June 2012 to January 2017, he served as Special Assistant to President Obama and as Cybersecurity Coordinator on the US National Security Council.

changing our mindset about how cyberspace works and creating a set of interlocking policies with different aspects, depending on the malicious actions being deterred. Implementing such expanded deterrence policies could generate substantial benefits for the digital ecosystem.

For many people, the term "deterrence" conjures up images of the Cold War and nuclear deterrence. Nuclear weapons are so destructive, so terrifying, that the primary goal for nuclear deterrence is zero use. The United States and its allies achieved that goal during the Cold War, and we have sustained that success so far in the 21st century. In fact, the resulting norm against nuclear weapon use is so deep-rooted that even non-state actors have largely shunned such capabilities, despite fears that the weapons would appeal to them. The success of nuclear deterrence means that all other deterrence efforts tend to be measured against it.

However, nuclear deterrence is not the right benchmark for cyber deterrence. First and foremost, zero use is not a realistic goal for cyber deterrence policies. The nature of cyber activities differs substantially from that of nuclear weapons; cyber effects are usually scalable, reversable, and vary widely in impact. Even nations that feel deeply about it cannot credibly threaten to conduct military strikes for low-level cyber espionage or extortion, nor does international law permit such disproportional responses. Further, the ability to confuse attribution, obfuscate activity, create ambiguity, and operate in an undetected manner makes complete deterrence infeasible. Finally, the motivations of cyber actors can differ substantially. Criminals are in it for the money, while nation-states are pursing national security goals. What deters money seekers is different from what deters security-minded government agencies.

As a result, even expanded cyber deterrence policies are not going to stop all malicious cyber activity. Such policies will not stop cyber-enabled espionage. They will not prevent nations from employing offensive cyber capabilities as part of their national security tool set, nor will they eliminate cybercrime from the Internet. A certain level of malicious cyber activity will be endemic to cyberspace, just like a certain level of malicious activity is endemic to the physical world. We can aim for world without the use of nuclear weapons; the same is not true for malicious cyber activity.

On the flip side, arguing that "deterrence" as a concept does not work at all in cyberspace ignores what already does not happen. Nations—such as the United States, the United Kingdom, Israel, China, Russia, and Iran—could use their offensive cyber capabilities to cause widespread disruption, even physical destruction, on a regular basis. For example, as part of its efforts to disrupt the Islamic state, the United States conducted cyber operations to disrupt their communications; the United States could regularly undertake such activities against foreign governments, if it so chose. The Russian government turned the power off in Ukraine in December 2015 and December 2016; they could choose to take such actions against power plants in other countries on a regular basis. If a criminal ransomware attack can shut down a manufacturer such as Norsk Hydro or a critical infrastructure such as the Colonial Pipeline, nation-states could use those capabilities much more often than they do. Yet, they do not.

Some restraint stems from economic self-interest, because most nations benefit from the economic activity that occurs in cyberspace. Another restraint comes from practicality, as cyber operations are more difficult to undertake than Hollywood movies portray. However, since nation-states sometimes use these capabilities, economic self-interest and technical difficulty alone are insufficient to explain the lack of offensive cyber activity. These nations choose not to use their offensive cyber capabilities in this manner partially because deterrence works—using such capabilities profligately would invite retaliation through a variety of means, including physical force. To explain the

relative paucity of disruptive or destructive nation-state cyberattacks, deterrence must factor into the explanation. Even cybercriminals try to maintain a degree of anonymity and avoid traveling to Western nations, so some minimal level of deterrence operates even against cybercrime.

Although some activities cannot be realistically deterred (such as espionage) and others are already deterred (e.g., nation-states undertaking widespread, frequent, destructive cyberattacks against critical infrastructure assets outside of armed conflict), a range of damaging malicious cyber activities falls in between these two types. Some nation-states and many criminal groups are exploiting this gap. These actors use cyber capabilities to cause physical disruption and harm, but not quite enough harm in any single instance that the United States or other countries have used military force to stop it. The cumulative nature of malicious cyber activity compounds the problems from the deterrence gap. Seen as individual actions, certain activity may seem to fall below the threshold of deterrability, but, when looked at in aggregate, the effects can be enormous. Ransomware is a good example. Although most individual ransomware attacks fall below the use of force as defined in international law, collectively ransomware attacks threaten our national security, economic prosperity, and public health and safety. Ransomware's aggregate burden is not sustainable over the long term at current levels.

The problem for cyber deterrence is not whether it works at all, but whether it can be expanded to work against a broader set of cyber activities and how to identify the activities that we want to deter.

Thus, the problem for cyber deterrence is not whether it works at all, but whether it can be expanded to work against a broader set of cyber activities and how to identify the activities that we want to deter. At present, the deterrence gap is big enough that activity falling within the gap is causing long-term harm to national security, economic prosperity, and public health and safety in both the digital and physical worlds. Therefore, the United States and like-minded nations should seek to implement a set of expanded cyber deterrence policies that shrink the size of the deterrence gap, reduce the volume, intensity, and impact of malicious cyber activity that falls within this gap, and reinforce agreed upon norms of behavior in cyberspace.

The United States and other nations have laid a good foundation for cyber deterrence policies through efforts to establish norms of acceptable behavior in cyberspace. Since 2013, with the agreement at the United Nations that international law applies in cyberspace and that states should adhere to eleven specified norms, international debate has focused on identifying specific actions that represent violations of those norms and how to enforce them. For the United States, its 2018 National Cyber Strategy articulated two concepts of deterrence, denial and cost imposition; the second concept is the method for holding norm violators accountable. This strategy provides a good scaffolding for deterrence policy. However, to expand cyber deterrence to better enforce the agreed upon cyber norms, all states that are serious in upholding these norms need not only to build out those concepts, but also—collectively—to think differently about cyber deterrence. Accordingly, the first step in expanding our deterrence efforts is to adopt new mental models.

Not surprisingly, the mental models most policy makers have for cyberspace are based on the physical world; after all, that world is what we experience. However, those mental models do not work well for cyberspace, because the physics and geometry of near light-speed, nodal networks and devices differ significantly from that of the continuous physical world. Any expanded cyber deterrence policies must adapt to these physical differences.

First, no locations exist in cyberspace outside the nodes; information packets can only move from one node to the next along predetermined paths. Packets cannot stop somewhere in the middle. Second, the structure of cyberspace means that concepts of "near" and "far" differ from those of the real world. Such concepts are defined by the route or path between nodes in the network, not by their physical location on earth. Thus, "proximity" also has a different meaning, depending on the path required to move between nodes. Third, fast and slow also have different meanings; "slow" on the Internet still generally means a vastly shorter time scale than in the physical world. Fourth, cyberspace borders are very different from physical borders. Contrary to the first three, this aspect of cyberspace geometry gets a lot of attention, the most frequently used adjective being "borderless." However, conventional wisdom gets this aspect wrong. Cyberspace is not, in fact, borderless. It has a plethora of borders, with every router, firewall, and network switch creating a boundary. The issue is not the lack of borders, but the fact that cyber borders do not align with the physical world's borders and boundaries. Further, cyber borders follow their own logic and rules, which do not necessarily comport with the nation-state political structures.

As an example of how these physical factors come together to render traditional policy approaches ineffective, take the idea of border control. In the physical world, national governments control (or try to control) the flow of people and goods into and out of their territories for many reasons, including safety and security. However, when governments try to provide "cyberspace border security" in a similar fashion, it usually does not work very well. Even China, with its Great Firewall, struggles with controlling information while still allowing the Internet to perform its economic functions. The reason for these failures flows directly from the physical structure of cyberspace. Since nodes have many connections and many paths for information to take, finding, designating, and controlling a consistent "border" is virtually impossible. A nation's cyberspace does not have a geometric shape with a defined edge and a large interior; it is a lattice of points or nodes, with the points connected to huge numbers of other points through an incomprehensibly complex network of paths. "Interior" is a meaningless concept.

At the same time, cyberspace is not entirely divorced from the physical world, operating on some separate ethereal plane. Although people often act as if cyberspace constitutes a separate reality, all the computers, routers, switches, servers, and Internet-of-Things devices exist someplace on the planet, almost always in some country's territory. As a result, while the "geography" of cyberspace differs from that of the physical world, it is not entirely separate from it either.

Once mental models change to account for the different physical characteristics of cyberspace, the second step is to apply the new models to traditional deterrence approaches to see what factors need to be accounted for. Conducting such an analysis reveals at least three factors that effective cyber deterrence policies must incorporate: the need to involve non-governmental actors, the overlapping combination of malicious cyberspace actors and their motivations, and the necessity of action.

In traditional deterrence models, governments are the only actors. Among other factors, such as technical capability, the nature of cyberspace borders requires us to expand our deterrence policies to encompass additional actors, including the private sector, non-profits, and individual citizens. If no "interior" exists in cyberspace, then every person, company, organization, and government occupies some portion of a cyber border. In turn, if every organization inhabits a cyber border, then governments cannot provide cyber "border security" on their own. Further, non-state actors dominate the cyberspace ecosystem, and the Internet itself is managed through a multistakeholder model. As a result, if we want cyber deterrence policies to expand into the gap, those policies

must involve many more players than just national governments. They must incorporate the private sector, cybersecurity providers, cloud service providers, telecommunication companies, international organizations, non-profits, civil society, and critical infrastructure owners and operators. Thus, the level of coordination and organization required for effective cyber deterrence policies is much higher than in traditional deterrence efforts. Getting all those divergent actors aligned with respect to goals and activities requires more time, effort, and energy than do traditional deterrence initiatives. The work of aligning these disparate groups' activities can be considered "operational collaboration." Since the government cannot compel collaboration (at least in the United States and most like-minded countries), such operational collaboration depends on nonstate actors' willing participation. Since we have not fully developed this concept of operational collaboration sufficiently to put it into practice, our previous efforts at deterrence have fallen short.

The second factor stems from the overlapping and sometimes ambiguous nature of the targets of deterrence. Traditional military or nuclear deterrence seeks to dissuade other national governments from undertaking certain military actions. It also typically focuses on an effectively small number of people within those governments. Traditional criminal deterrence is most frequently domestically focused, aimed at actors that are exclusively criminals, and spread broadly across a population. For cyber deterrence, the situation is more complex. The line between nation-state and criminal actors has become very blurred in cyberspace, whether due to the use of criminal groups as proxies (in the case of Russia) or because the government is carrying out criminal activities to circumvent international economic sanctions (in the case of North Korea). As a result, the elements related to national governments and criminals are intermixed. At the same time, though, nation-states and cybercriminals undertake malicious cyber activity for fundamentally different reasons.

Cyber deterrence policy must deal with these different motivations simultaneously. Yet, deterring someone who is seeking money is very different than deterring someone who is personally committed to advancing a cause. Actions that choke off financial flows might deter a money-seeking cybercriminal, but will not dissuade a hacktivist. Cybercriminals spend a very limited amount time or resources trying to access any given target's network. If it proves too difficult or time-consuming, they move on to other, easier-to-access victims. Accordingly, deterrence by denial often proves highly effective against cybercriminals. A nation-state, however, can be much more patient, biding its time, and expending many more resources to access a given target if they need to access that target to advance their national-security goals. Given the intertwined nature of malicious cyber actors, expanded cyber deterrence must combine policy components from military and criminal deterrence with approaches that are aimed at deterring different motivations, depending on the specific situation.

To date, the United States and its allies have not clearly tied deterrence efforts to behavioral benchmarks.

Based on this logic, the United States and those states interested in upholding the agreed norms should broaden the variety of tools used to impose different kinds of costs on the adversaries. Focusing on only one kind of cost imposition, such as an overwhelming military response or a technical cyber response, will not credibly deter as broad an array of malicious cyber actors as needed. Interlocking, multi-faceted cyber policies will have many different cost imposition elements, each aimed at a different type of malicious behavior.

Finally, cyber deterrence requires action. Nuclear deterrence relied on the threat of action, but it did not require demonstrations in the physical world to be credible. Since the potential damage from

nuclear weapons was so vast and irreversible, the threat of credible retaliation was sufficient. In fact, with zero use as the goal, the less action and the less direct confrontation, the better, as far as traditional deterrence initiatives were concerned. Nuclear weapons use was and remains binary—either they are used or not. They only result in permanent destruction and any individual weapon cannot be scaled up or down in destructiveness.

This situation is reversed for cyber deterrence. Malicious cyber action is not binary; it is often reversible, and frequently scalable, with a wide array of consequences. As a result, the mere threat of action is not sufficient to expand deterrence into the gap. Thus, enhanced cyber deterrence policies will involve action and retaliation. Such actions do not have to involve the use of military force or even military components at all, although they can. Diplomatic, law enforcement, technical counter-cyber operations, and economic penalties should also form part of that array.

With a revised mental model in place and key policy factors incorporated, the third step in expanding cyber deterrence is identifying policy design differences from traditional or current deterrence efforts. Specifically, expanded cyber deterrence policies should differ in five ways: clearly defining the new activity to be deterred, making use of comparative advantage, linking cyber issues with non-cyber issues explicitly, encompassing more than technical cyber actions, and involving active disruption.

While some ambiguity can be helpful in deterrence, too much ambiguity reduces its utility. To date, the United States and its allies have not clearly tied deterrence efforts to behavioral benchmarks. Such benchmarks would not constitute redlines (as in, if you do x, we will do y), but rather an articulation of what malicious cyber activities the United States and its allies seeks to deter beyond what is already deterred. Thus, the first design difference would be to tie expanded deterrence policies to specific behaviors. Already agreed upon international norms of behavior, such as the eleven United Nations norms or those proposed by the Global Commission on the Stability of Cyberspace, provide a tailor-made set of behaviors to incorporate into an expanded deterrence policy design. Reducing ambiguity in behavior that the United States and its allies want to deter does not require committing to a specific action in response to such behavior, but effective deterrence does require a consistent overall response to such activities.

The second design difference lies in identifying an organizing principle for the effort. Since expanded cyber deterrence policies will rely on operational collaboration among a broader array of actors than will traditional deterrence activities, the challenge becomes one of building, organizing, aligning, and sustaining that collaboration. Trust is an oft-discussed ingredient of such collaborative efforts, and it is extremely important. However, a second, less examined enabling principle should be comparative advantage. Specially, cyber deterrence efforts should explicitly consider which private sector or non-profit organizations have the comparative advantage in a given task or function, and governments should closely examine where their comparative advantage lies.

Cybersecurity vendors can bring their technical understanding of how networks and devices function to shape operations, and their intelligence to help identify targets. Internet Service Providers, Cloud Service Providers, and Hosting Providers can focus on disrupting the adversary's technical infrastructure. Civil society and non-profit information sharing and analysis organizations can play connective roles, bringing together the disparate players and ensuring a broader picture of what is occurring. Governments should focus on adding context derived from intelligence and taking direct action against malicious actors. By leveraging different organizations' comparative advantages, a wider approach to cyber deterrence would have a multiplier effect, where the sum is

much greater than the individual parts. For governments, a significant challenge is engaging these nonstate actors in a way that does not treat them as subordinates, but as partners. Fortunately, many organizations already are convinced of the need for concerted international and multistakeholder actions to uphold norms of good behavior in cyberspace, and they are waiting for an appropriate engagement forum to emerge. The recently concluded first round of the United Nations First Open-Ended Working Group (OEWG) on the challenges of ICT in the context of international security demonstrated how important it is to reach out to nonstate actors.

Since the impact of malicious cyber activity is not constrained to cyberspace, efforts to deter such activity should not be confined to cyberspace either. Thus, cyber deterrence policies should explicitly link cyber issues, such as harboring cyber criminals, with non-cyber issues that the target nation cares about. For example, if Nation A wants support for a resolution on topic "x" at the United Nations and that nation is well-known for harboring cyber criminals, then other nations should require a decrease in malicious cyber activity emanating from Nation A's territory. Such linkages would be consistent with the international law principle of effective control; under this concept, governments are obliged to address criminal activity that emanates from their territories. The Obama Administration learned a similar lesson in linking cyberspace to the physical world when dealing with China's theft of intellectual property; only after the United States was willing to connect that issue with other issues in the relationship, and raise it continually through every channel possible, did China formally agree to limit such activities. Linking cyber deterrence to broader geo-political relationships and actions will increase the ability to shrink the gap and reduce activity.

Effective cyber deterrence requires integrating non-cyber tools, such as diplomacy, economic sanctions, financial system constraints, civil legal processes, law enforcement action, and even military action.

As many cyber policy experts have noted, malicious cyber activity should not be met only with cyber-based responses. This aspect forms the fourth design difference from traditional nuclear deterrence. Effective cyber deterrence requires integrating non-cyber tools, such as diplomacy, economic sanctions, financial system constraints, civil legal processes, law enforcement action, and even military action. Technical cyber actions will certainly be a part of the tool set, but will only form a small part of it. Thus, cyber deterrence policies will employ a wide range of tools, selecting the tools that will have the greatest effect on the intended target. Since cybercriminals are motivated primarily by money, focusing on bringing the cryptocurrency exchanges into compliance with global financial rules could be a very effective tool against them. On the other hand, a nation-state actor might be more concerned with diplomatic losses.

Finally, effective cyber deterrence policies will require regular, sustained disruption of malicious cyber activity. Such disruption should be technical, logistical, legal, financial, diplomatic, and, if necessary, kinetic. Increasing the scope, scale, and cadence of disruption activities would impose real costs on our common adversaries; given the level of malicious activity currently occurring, deterrence will not be credible unless it is backed by clear, decisive action. Further, rather than reaching a steady end-state, cyber deterrence policies should seek to push the digital ecosystem into a dynamic equilibrium. Activity would occasionally increase, necessitating stepped up disruption activity; at other points, activity would drop below the equilibrium level, allowing nations to shift some resources to other problems.

If the United States, its allies, and like-minded nations were to deploy expanded cyber deterrence policies with these five features, doing so could achieve two strategic goals. First, the cyber deter-

rence gap would shrink, effectively expanding the range of deterrable activity. Second, the volume, intensity, and impact of malicious activity that falls within that narrower gap would be reduced.

Counterintuitively, these expanded cyber deterrence policies could narrow the deterrence gap by more clearly defining the acceptable uses and effects of offensive cyber capabilities. Cyber deterrence allows for such a possibility precisely because it does not seek zero use, but instead aims for risk management. By gaining broad agreement on the acceptable uses for offensive cyber capabilities outside of active armed conflict, the inverse would also be true: we would have a better understanding of the actions and effects that are outside the bounds. Such an outcome would enable countries to understand and plan for how offensive cyber operations might be used, and it would provide a benchmark against which to measure nations and other actors. This outcome would also allow like-minded nations to protect not just critical infrastructure services or property from cyber operations, but also to protect other kinds of activity, such as democratic elections. Since not just governments, but a broad, multi-stakeholder coalition would have helped create these definitions, the ability to take legitimate action against those entities pursuing "out of bounds" activities would increase.

These expanded, interlocking cyber deterrence policies would also reduce the level of malicious activity endemic to the digital ecosystem. While the United States and its allies cannot eliminate malicious cyber activity, they can reduce such activities to a manageable level over the long run. Expanded cyber deterrence policies could help achieve this goal by reducing criminal safe harbors, the impact of ransomware, and the use of proxies.

Expanded cyber deterrence policies would shrink the number of countries harboring cybercriminals in two ways. Capacity building already forms a part of cyber deterrence; enhanced policies would dramatically expand these efforts. Therefore, if a country lacks the technical capability to pursue, arrest, and prosecute cybercriminals, then a combination of private sector, NGO, and foreign government resources would provide a backstop. On the other hand, if a country currently perceives harboring criminals as beneficial, then cyber deterrence policies that are more tightly coupled to other, non-cyber interests will alter that calculus. Instead of seeing cybercriminals as a cost-free augmentation of government capabilities, the country would take on some liabilities.

Ransomware has transitioned from an economic nuisance to a national security and public health and safety threat. The level of economic damage, the resources now financing other criminal activities, and the impact to public health and safety have become too large to sustain. Cyber deterrence can play a role in combating this growing threat. As with malicious cyber activity more broadly, cyber deterrence might seem useless against ransomware attacks. However, the multistakeholder Ransomware Task Force sponsored by the Institute for Security and Technology recently released a report with almost fifty policy recommendations for reducing the scope, scale, and impact of ransomware; almost a quarter of these recommendations focused on using deterrence against ransomware. Along with preparedness, disruption, and response, deterrence was one of the four main policy areas in the report. The Task Force embraced deterrence not only as a possibility but as a critical element in the fight against ransomware.

Finally, expanded cyber deterrence policies could help disentangle cybercrime from nation-state activity by discouraging the use of proxies. Since the United Nations Group of Governmental Experts issued its consensus report in June 2013, many governments have come to agree that one norm of responsible behavior in cyberspace is that countries are responsible for malicious cyber activity emanating from their territory, regardless of whether they are aware of such activity before

it occurs. Expanded cyber deterrence policies tied more explicitly to these norms would increase international and multistakeholder pressure on nations to reduce the use of proxies. Coupled with better definitions of acceptable behavior, the ability to use "plausibly deniable" proxies would decrease because nations would be responsible for such behavior. By holding nations more accountable for damages, even if unintended or stemming from supposedly non-state actors, a cyber deterrence initiative could constrain the more profligate use of proxies. This constraint would also encourage nations to be more targeted and cautious in their use of cyber tools, and in turn reduce the impact of these operations on the ecosystem.

As the digital ecosystem becomes ever more integral to the functioning of societies around the world, establishing effective cyber deterrence policies becomes a critical, even existential requirement. Although some scholars have argued that we should abandon the concept of deterrence in cyberspace, without effective deterrence policies cyberspace will become a net liability rather than an asset. The good news is that, while it does not work in the same manner as nuclear deterrence, cyber deterrence already works to some degree. The United States and like-minded nations intent on upholding the agreed norms need to expand deterrence's reach, stopping more malicious cyber activity before it occurs, and they need to reduce the impact of any remaining activity to sustainable levels. Sustained, coordinated cyber deterrence policies that properly account for cyberspace's nature and that have the characteristics outlined above would enable the United States and its allies to better enforce the already agreed to norms of behavior in cyberspace. It could also reduce the impact of cybercrime on our economies and public health and safety. Such an effort can work, but it can only do so through sustained, high-level commitment, and a realization that we cannot solve our cybersecurity problems, we can only manage their risks. But managing those risks effectively would generate huge benefits for everyone.

Endnotes

1 For example, see Richard J. Harknett and Michael P. Fischerkeller. "Deterrence is not a credible strategy for cyberspace." Orbis, June 23, 2017. https://www.fpri.org/article/2017/06/deterrence-not-credible-strategy-cyberspace/.

2 Dina Temple-Raston. "How the US Hacked the ISIS." National Public Radio, September 26, 2019. https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis.

3 The United States Department of Justice. "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace." Office of Public Affairs, October 19, 2020. https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

4 Bill Briggs. "Hackers hit Norsk Hydro with ransomware. The company responded with transparency." Microsoft, December 16, 2019. https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/.

5 David Sanger and Nicole Perlroth. "Pipeline Attack Yields Urgent Lessons Abour US Cybersecurity." New York Times, May 14, 2021. https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html.

6 United Nations General Assembly. Developments in the field of information and telecommunications in the context of international security. December 27, 2013. https://undocs.org/A/RES/68/243.

7 The White House. "National Cyber Security Strategy of the United States of America." September 2018. https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

8 The Aspen Institute's Cybersecurity Group published elaborating on this concept: "An Operational Collaboration Framework." Aspen Cybersecurity Group, November 2018. https://www.aspeninstitute.org/publications/an-operational-collaboration-framework/.

9 Add the following reference to endnote ix for that May 2021 GGE report: https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf; The Global Commission on the Stability of Cyberspace. Advancing Cyberstability. The Hague: The GCSC, November 2019. https://cyberstability.org/report/.

10 The White House Office of the Press Secretary. "Fact Sheet: President Xi Jinping's State Visit to the United States." Last Modified September 25, 2015. https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

11 The Institute for Security+Technology. "RTF Report: Combatting Ransomware." Accessed June 17, 2021. https://securityandtechnology.org/ransomwaretaskforce/report/. The Task Force brought together more than 60 people from the private sector, civil society, sharing organizations, and governments for a three month sprint to develop these recommendations.

12 United Nations General Assembly. "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." June 24, 2013. https://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-tele- communications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-518.pdf.

About the Author

Michael Daniel serves as the President & CEO of the Cyber Threat Alliance (CTA), a not-for-profit that enables high-quality cyber threat information sharing among cybersecurity organizations. Prior to CTA, Michael served for four years as US Cybersecurity Coordinator, leading US cybersecurity policy development, facilitating US government partnerships with the private sector and other nations, and coordinating significant incident response activities. From 1995 to 2012, Michael worked for the Office of Management and Budget, overseeing funding for the U.S. Intelligence Community. Michael also works with the Aspen Cybersecurity Group, the World Economic Forum's Partnership Against Cybercrime, and other organizations improving cybersecurity in the digital ecosystem. In his spare time, he enjoys running and martial arts.

Cyberstability Paper Series

New Conditions and Constellations in Cyber

A Chinese Perspective on the Future of Cyberspace

Xu Peixi
Professor & Director of Global Internet Governance Studies Center,
The Communication University of China

A Chinese Perspective on the Future of Cyberspace

Xu Peixi | Professor & Director of Global Internet Governance Studies Center, The Communication University of China

Internet governance has moved beyond a narrow technical dimension of the early days and come to include all the key social topics, ranging from the digital economy, technological innovation, and military modernization, to political stability. It compasses all the stakeholders of the state, private sector, and civil society, and involves all the government institutions from commerce to defense. While the Internet empowers the grassroots and creates new opportunities for social justice, it is increasingly being haunted by military adventures, power competitions, disinformation campaigns, and financial fraud. Luckily, the plurality of relevant actors in cyberspace means that many of the proposed norms on regulating cyber behavior have wider appeal than it may seem.

This article firstly discusses how China perceives external threats, and observes that history or sovereignty is China's dominant perspective about cybersecurity. Then, it points out the fact that China is the most dependent country on the digital economy, and development is the dominant perspective in that field. It argues that China's worldview about cyberspace is reflected in its Confucian and Daoist traditions, and recommends a transnational and pluralistic approach to looking at cyberspace. It concludes with an analysis of several developing cyber norms.

In terms of security, a dominant Chinese perspective about cyberspace has been shaped and predetermined by past historical experiences and memories inherited and projected from the agrarian and industrial ages. This can be said to be a Chinese perspective about cybersecurity, under which cyberspace is a new domain where external threats originate.

Xu Peixi is Professor and Director of the Global Internet Governance Studies Center at the Communication University of China (CUC). He is an active participant of IGF and China-EU, China-U.S. cyber dialogues.

In agrarian centuries, external threats mainly came from the land, and nomads in the territories north and west of the Great Wall had a natural tendency to execute large-scale invasions in times of bad weather and in periods of China's disunity. The need to exercise national defense against nomads is one of the three factors ruling out the possibility of a decentralized China, in addition to the necessity to tame the Yellow River and the obligation to commit vast resources to save people and regions struck by drought and flood caused regularly by fluctuations in the monsoon rainfall. Against such a backdrop, a unified China was born as early as 221 BC, and this feature of early unification and centralized governance serves as the sole and most evident difference between Chinese and European cultures. From then on, unity, oneness, and harmony as important Chinese cultural values have been emphasized.

Over the industrial centuries, major threats were from the sea, and China was repeatedly defeated by European and Japanese powers. The one hundred years, from the 1840s to the 1940s, of foreign subjugation and occupation is referred to as the "era of national humiliation" in history discourse and political rhetoric. The desire to account for this is reflected in the first words of the Chinese national anthem, which call on China to "stand up."

In terms of security, a dominant Chinese perspective about cyberspace has been shaped and predetermined by past historical experiences and memories inherited and projected from the agrarian and industrial ages.

In the digital age, cyberspace has been added as a new frontier where external threats against China's integrity and unity originate. At the beginning, cybersecurity was understood from an information security perspective. The online content filtering system known as the Great Firewall started to operate in 2003. The 2013 Snowden leaks made China aware of the fact that Chinese targets—ranging from private companies such as Huawei, to universities such as Tsinghua University, to the very top of China's leadership, China's President—are vulnerable to foreign intelligence agencies.

It was within this context that institutional reforms were made and the Leading Small Group for Cybersecurity and Informatization was established in 2014, representing a distinctive shift of approaching Internet issues from a perspective of economic growth and content challenges, in addition to that of infrastructure security. In December 2015, the Chinese President, Xi Jinping, proposed the notion of cyber sovereignty as a response to external cyber threats.

Development is the dominant perspective when looking at the Chinese economy in general and the digital economy in particular. On 20 September 1987, China successfully sent the first email to Germany, entitled "across the Great Wall we can reach every corner in the world." On 20 April 1994, China achieved full-functional connection to the Internet by opening a line through Sprint Co. Ltd. The Internet was introduced into China in the late 1980s and early 1990s, in a social background with two distinct features.

Firstly, the first unique feature was the rise of the grassroots user base. Decades of radical revolutions and social movements had flattened the traditionally hierarchical Chinese society and removed the ropes and chains binding the people, such as imperial authority, clan authority, religious authority, and patriarchal authority. Radical revolutions went to such extremes that traditional hierarchical codes were abolished, Buddhist temples were torn down, family-tree books were burned, and worship of ancestors was abandoned. Most effective of all, gender equality has been legally guaranteed. Without these steps, it is difficult to imagine that a grassroots user base—with the Internet being available to the common people—would have been possible at all.

A second feature was the rise of the market. The Third Plenary Session of the 11th Central Committee held in 1978 paved the way for the installation and prosperity of market mechanisms, in pursuit of modernization. Private ownership was acknowledged and legally regulated. Economic development was the new logic of social evolution. As a result, China entered a massive economic growth phase unlike anything in human history. Chinese society is therefore undergoing a rapid transition on three levels: the agrarian level, the industrial level, and the informational level. Unlike with advanced Western economies in which the industrial phase alone took three centuries, the two transitions on the three levels have been happening simultaneously in China over the last four decades.

It was against this social background, featured by the co-rise of the grassroots user base and the market, that the Internet was introduced into China in the late 1980s, where it unleashed waves of innovations and changes that are arguably deeper than that which has been witnessed elsewhere. Led by the Internet and new ICTs, and globally integrated into the world economy through trade regimes such as the WTO, these innovations have nurtured the emergence of scores of leading companies. This includes the manufacturer Huawei, technology conglomerate Tencent, electronics company Xiaomi Inc., and also Internet giants such as the Internet search engine Baidu, e-commerce giants Alibaba and JD.com, the online content platform ByteDance, life service platform Meituan, ride-sharing giant Didi, microblog social network Sina Weibo, and video-hosting service Youku Tudou, among others.

These domestically or locally dominating technology companies, together with a plethora of other digital businesses, are defining the digital lifestyles of nearly one billion Chinese Internet users. China's digital economy was valued at 39.2 trillion Yuan (approximately 6 trillion USD) in 2020, accounting for 38.6 percent of the GDP of the same year, and from that perspective making China the most dependent country on the digital economy. This pursuit for digital prosperity serves as the economic reason for China's vision about building "a community of shared future for mankind in cyberspace." This makes China the least willing and the most anxious to see signs of fragmentation of the Internet, and a potentially strong supporter of many developing cyber norms proposed by state or non-state actors as diverse as Microsoft Corporation, the Global Commission on the Stability of Cyberspace, the Carnegie Endowment for International Peace, the Internet & Jurisdiction Policy Network, French President Emmanuel Macron, and Internet pioneer Tim Berners-Lee.

In contrast to the Chinese perspectives of approaching cybersecurity from history or from a sovereignty perspective, and approaching the digital economy from a development or globalization perspective, a typical Western way of addressing cyberspace, however, often seems viewed through a lens of good guys versus bad guys, or even good versus evil. While the Chinese viewpoint sees itself as essentially pragmatic, it often considers the Western viewpoints to be essentially moralistic, at best. From the 2017 Trump Administration onwards, this worldview of good guys versus bad guys has become increasingly salient and has been translated into concrete digital policies, driving global Internet governance into a downward spiral of fragmentation and foreseeing a scenario of a digital Cold War.

Represented by the *Clean Network Initiative*, a systematic and historically unprecedented intervention in the global supply chain is taking place. This not only interrupts the roll-out of 5G, seen as being an important technological development, but also other cutting-edge technologies. These anti-trade measures are gaining momentum and casting divisions in the global Internet ecosystems at the cost of global businesses.

Numerous proposals and initiatives demonstrating the good-guys-versus-bad-guys perspective are being made. Nations as diverse as Russia, China, Iran, and North Korea are conveniently categorized together by a plethora of politicians, think tankers, and sometimes even by academia, and packaged into enemies, bad guys, adversaries, or, at best, as competitors. These voices claim to warn about "the rise of digital authoritarianism." China was labeled as representing a "digital authoritarian model" and was constantly accused of spreading "authoritarian tech." At the same time, the EU and the United States are called upon to work on "countering digital authoritarianism" and "addressing China together."

The increasing popularity of the rhetoric happens before a backdrop of rising geopolitical tensions in the digital and non-digital realms. But the terminology is not new. Broadly, it resembles a digital rearticulation of a mixture of Orientalist imaginations, a Cold War ideological framework, and a Huntington lens of civilizational clashes.

Specifically, it is a digital rebirth of *Four Theories of the Press*: authoritarian theory, libertarian theory, social responsibility theory, and Soviet Communist theory, which were written in the years of the Cold War. All the good virtues, such as libertarianism and social responsibility, are owned by the West. All the bad characteristics, such as authoritarianism and Soviet Communism, are attached to the others. The Four Theories framework of thinking had influenced media and communication learners for decades before it was systematically reflected and fundamentally challenged, in *Media, Messages, and Men, Agents of Power, Last Rights: Revisiting Four Theories of the Press,* and *Normative Theories of the Media.*

Rather than applying the good-guys-versus-bad-guys perspective, it would be more appropriate to argue that all societies and cultures have both authoritarian and libertarian orientations in handling the mixed security and development challenges posed by cyberspace, and each orientation occupies a position in the libertarian-authoritarian continuum.

Under such a thought experiment, the United States as a nation in itself owns the most authoritarian and the most libertarian elements of Internet governance, occupying the two ends of the continuum. The U.S. military and NATO, located in the far left of the continuum, are, knowingly or not, shaping the most authoritarian elements of Internet governance, by imagining enemies or adversaries that need combatting. On the other side, the U.S. IT sector, Silicon Valley, and Internet technical communities, located in the far right of the continuum, are promoting the most libertarian version of Internet governance. They represent two contradictory values and practices, and their ways of cooperation and competition in the digital age would, to a large extent, decide the fate of the Internet. There has never been a singular value about cyberspace, even in the United States itself—the birthplace of the Internet.

While the Chinese viewpoint sees itself as essentially pragmatic, it often considers the Western viewpoints to be essentially moralistic, at best.

The same may also be true about China, which has its authoritarian and libertarian traditions that are represented by Confucianism and Taoism. They are the hidden codes that guide thinking about old fields and new domains. Taoism and Confucianism are both opposites and complementary. Xiao summarizes: "Whereas Confucius and Mencius, one of the foremost Confucian thinkers, promoted moral cultivation and a hierarchical system of human relations as solutions to the social chaos of their times, the founders of Taoism, the mythical Laozi and Zhuangzi, viewed such moral and social efforts as artificial constraints on the very nature of human beings and the *Tao* (Way) of the universe.

Laozi and Zhuangzi advocated the idea of *wuwei* (effortless action), which has led to Taoism being associated with the themes of naturalness, spontaneity, relatedness, pluralism, anarchism, and laissez-faire government."

Chen observes that the fundamental difference between Confucianism and Taoism is that they evolve respectively into the ideological agents of state actors and non-state actors, and the former often serves a restricting role, the latter an intriguing and liberating role. The early days of Internet growth were an annotation of a Taoist approach. "Its development was driven by non-governmental developers, providers, and users of the new services." "Internet standards, codes, and guidelines...came not top down by majority voting of elected parliamentarian representatives, but were drafted bottom up by the respected and competent key players of the global Internet community."

As cyberspace evolves to include more stakeholders, tensions between different pillars of society exist. State, commercial, and grassroots logics meet, expand, interact, and compete in the new domain. Domestic disagreements between different actors about how the Internet should be governed are no less evident than in the global arena.

As one example, the private online video platforms did not rise and succeed in China overnight. They survived a most tightly regulated broadcasting sector, and it took many struggles to push back China's state efforts to have them nationalized. As another example, the cities of Beijing and Shenzhen have drastically different ride-sharing policies, reflecting different local priorities. In terms of the grassroots Internet financing industry serving a completely new consumer credit market, there have been rising tensions between the new companies and vested interests in the state-controlled banking sector.

Together with all the domestic and geopolitical realities, cyberspace differs from many other domains in that it covers a whole spectrum of dimensions, and these dimensions are interconnected and intertwined due to the oneness nature of the global Internet. Under the circumstance, globally speaking, it is difficult to repeat the successes in nuclear weapons (*Treaty on the Non-Proliferation of Nuclear Weapons*), sea (*United Nations Convention on the Law of the Sea*), and climate change (*Paris Climate Agreement*). The current fragmented landscape of cyber and digital dialogues will continue for longer than perhaps was originally hoped by early observers.

However, in spite of the challenges and frustrations, global efforts to reach agreement on certain cyber norms are delivering positive results. States, businesses, and civil society actors are seeking global solutions. In December 2014, Microsoft proposed six cybersecurity norms. In November 2018, the Global Commission on the Stability of Cyberspace issued its final version of an eight-norms package. Many of these norms were already referenced in the nine principles of the Paris Call.

In July 2019, Tim Berners-Lee published the first draft text of the Contract for the Web, proposing eight principles by which to save the Internet. In September 2020, Chinese Foreign Minister Wang Yi launched *Global Data Security Initiative*, outlining eight principles calling for a facts-based approach instead of an ideological one, by which to solve global data disputes. In March 2021, the OEWG 2019-2020 published its final report. In May 2021, the UN GGE 2019-2020 adopted a consensus report.

While the above-mentioned initiatives reveal quite different understandings about cyberspace, they contain many vivid details and, most important of all, they aim at seeking global solutions rath-

er than at just making accusations. State and non-state stakeholders' positions regarding cyber espionage, the public core of the Internet, cross-border content, and cybersecurity vulnerability, are gaining visibility. Most tellingly, a number of seemingly very different norms have turned out to be closer to each other then they had originally seemed.

These norms-building processes, with varying degree of success, underline a consistent and constructive thread in the global cyber dialogue. They persist in seeking global solutions and refuse to be carried away by increasing geopolitical tensions. Within the processes, actors from technical and political backgrounds meet, stakeholders from security and business circles communicate, and people with idealistic and realistic viewpoints cooperate.

The first example is the so-called Cyber Espionage Norm. On 25 September 2015, China and the United States came to an understanding about cyber espionage activities. The norm limits the activity of espionage in that it disavows intellectual property thefts by military and intelligence agencies "for intent of commercial advantage," while not addressing other forms of espionage. The norm was reconfirmed also between China and Britain (2015), the United States and India (2016), and China and Canada (2017), and was found in Group of 20 (2015) and Group of 7 (2017) outcome documents. It is also one of the nine principles of the *Paris Call* (2018). The most salient feature of the original Xi-Obama agreement is that it protects the vulnerabilities of the industry but does not weaken the strengths of the intelligence actors on either side. By that token, the norm symbolizes a win-win result, perhaps not just between China and the United States, but also between the industry and intelligence agencies.

The second example is the Non-Interference with the Public Core of the Internet Norm. On 21 November 2017, the Global Commission on the Stability of Cyberspace (GCSC) issued a call to protect the public core of the Internet. The norm started as a report submitted in March 2015 to the Dutch Ministry of Foreign Affairs. "Its main argument is that the Internet's infrastructure and core protocols should be regarded as a global public good that is in need of protection against unwarranted interventions by states and other parties."

The norm is similar to the cyber espionage norm in wording, and it nevertheless implies a message that penetration into undersea cables is permitted as long as it does not cause tangible damages. On the other hand, the most valuable part of the norm is that it may help to reduce the anxieties of many non-Western nations about the theoretical possibility that their country code top-level domains, such as .uk, .de, or .cn, might be removed from cyberspace.

The norm's association with global public good does not appear in the final report of the GCSC, but does appear in the 2019 *EU Cybersecurity Act*, which states: "The public core of the open internet, namely, its main protocols and infrastructure, which are a global public good, provides the essential functionality of the internet as a whole and underpins its normal operation. ENISA should support the security of the public core of the open internet and the stability of its functioning, including, but not limited to, key protocols (in particular, DNS, BGP, and IPv6), the operation of the domain name system (such as the operation of all top-level domains), and the operation of the root zone."

China's diplomatic position about the public core norm remains hesitant and unclear. In a statement about the initial pre-draft of the OEWG report, China comments that the concept "has not gained global consensus yet." However, the norm, particularly the *EU Cybersecurity Act* version that brings back the phrase "global public good," gives a firm commitment about cyber stability and should be welcome in China.

The third example is the Vulnerability Norm. In December 2014, Microsoft published *International Cybersecurity Norms: Reducing Conflict in an Internet-Dependent World*, and proposed six bold norms to limit conflict. The first norm proposed that states should be prohibited from inserting vulnerabilities or backdoors. The Microsoft proposal turns out to be the most prohibitive norm among similar proposals.

In contrast, the GCSC's proposal about the vulnerability norm is not as restrictive. It says that "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 norm singles out the development and production phases and, meanwhile, the norm implies that even the development and production phases can be tampered with, if the action does not impair cyberstability.

The public core norm, particularly the *EU Cybersecurity Act* version that brings back the phrase "global public good", gives a firm commitments about cyber stability and should be welcome in China.

Chinese legal language often indirectly indicates a prohibitive signal about inserting backdoors by state actors. However, China's *Global Initiative on Data Security* does not mention how state actors should behave, but makes it clear that "ICT products and services providers should not install backdoors in their products and services to illegally obtain users' data, control or manipulate users' systems and devices."

The fourth example is the norm to not use ICTs to interfere with the internal affairs. On 9 January 2015, the Shanghai Cooperation Organization (SCO) proposed the *International Code of Conduct for Information Security* to the United Nations, pinpointing such a wording about ICTs and internal affairs.

The SCO proposal is broad and contains both technical and content elements, but tilts more toward content. It has something in common with the suggestion in the *Tallinn Manual 2.0* that cross-border propaganda may constitute a violation of sovereignty if it incites turmoil. Seeing itself as a victim of decades of one-way flow of information, China is more than willing to further define norms in this aspect.

The proposed norms in this area are either technically focused or content focused. A pure content perspective is reflected in Article 20 of the *International Covenant on Civil and Political Rights*, prohibiting "any propaganda for war" and "any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence," and the digital application of this international legal instrument is inspiring the cross-border content moderation working group at the Internet & Jurisdiction Policy Network, based in Paris.

GCSC represents a technical perspective when proposing a norm to protect electoral infrastructure, saying, "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."

The above norm-building processes show that, even though there may be very different motivations for actors to propose or agree upon a specific norm, in technical detail and outcome they may be more alike. This realistic, pragmatic, yet global way of approaching cyber challenges increases the odds of finding commonalities between different states, stakeholders, and cultures, reduces the scenario of a digital Cold War, and pushes global Internet governance toward a digital commons, similar to the current direction in which global co-operation on climate change is heading.

Endnotes

1 Ray Huang. Broadening the Horizons of Chinese History. New York: M. E. Sharpe, Inc. 1999. 29.

2 Ibid. 23.

3 Larry A. Samovar, Richard E. Porter, Edwin R. McDaniel, and Carolyn S. Roy. Communication between Cultures (9th Edition). Boston: Cengage Learning, 2017.174.

4 For instance, the 1950 People's Republic of China Marriage Law was the first law introduced by the newly founded Republic. See Chen Xinxin. "Marriage Law Revisions Reflect Social Progress in China." China Today, April 2001. https://web.archive.org/web/20100629155714/http://www.chinatoday.com.cn/English/e2001/e200103/hunyin.htm.

5 China Digital Economy Development White Paper. China Academy of Information and Communications Technology, April 2021. 5.

6 United Nations General Assembly. Developments in the field of information and telecommunications in the context of international security. UN GA, October 2020. https://www.reachingcriticalwill.org/images/documents/Disarmament-fora/1com/1com20/resolutions/L8Rev1.pdf.

7 See "The Rise Of Digital Authoritarianism: China, AI, & Human Rights," a seminar series ran from September to October 2020 by the Hoover Institution. Accessible at https://www.hoover.org/events/rise-digital-authoritarianism-china-ai-human-rights.

8 See "A Transatlantic Effort to Take on China Starts with Technology," a virtual event ran by CEPA. Accessible at https://cepa.org/event/a-transatlantic-effort-to-take-on-china-starts-with-technology/.

9 See the "#DefendDemocracy"virtual series, ran by the Alliance of Democracies. Accessible at https://www.allianceofdemocracies.org/initiatives/the-campaign/defenddemocracy-virtual-series/.

10 See the "EU-US Future Forum," a virtual forum ran by the Atlantic Council from May 5-7, 2021. Accessible at https://www.atlanticcouncil.org/programs/europe-center/eu-us-future-forum/.

11 Fred S. Siebert, Theodore Peterson, and Wilbur Schramm. Four Theories of the Press. Urbana: University of Illinois Press, 1956.

12 Merrill and Lowenstein. Media, Messages, and Men: New Perspectives in Communication. New York: David McKay Company Inc,1979.

13 Herbert Altschull. Agents of Power. New York: Longman, 1984.

14 John C. Nerone. Last Rights: Revisiting Four Theories of the Press. Urbana: University of Illinois Press, 1995.

15 Clifford G. Christians, Theodore L. Glasser, et al. Normative Theories of the Media. Urbana: University of Illinois Press, 2009.

16 Xiao Xiaosui. "Taoist Communication Theory" in Encyclopedia of Communication Theory edited by Stephen W. Littlejohn and Karen A. Foss. Thousand Oaks: Sage Publications, 2008. 955.

17 Chen Guying. New Comments on Laozi & Zhuangzi. Bejing: ZHONGHUA Book Company, 1991. 4.

18 Wolfgang Kleinwächter. "200 Years of Negotiation on Cross-Border Communications: From Intergovernmental Treaties to the Multistakeholder Model for the Governance of the internet" in Towards Equity in Global Communication? edited by Richard C. Vincent and Kaarle Nordenstreng. Cresskill: Hampton Press, 2016. 129.

19 GCSC. Norm Package Singapore. GSCS: The Hague, November 2018. https://cyberstability.org/wp-content/uploads/2018/11/GCSC-Singapore-Norm-Package-3MB.pdf.

20 Paris Call. "The 9 Principles," accessed June 22, 2021. https://pariscall.international/en/principles.

21 Berners-Lee, Tim. "Contract for the Web,"Contract for the Web, accessed June 22, 2021. https://contractfortheweb.org/#main.

22 Ministry of Foreign Affairs for the People's Republic of China. "Global Initiative on Data Security,"last modified September 8, 2020. https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1812951.shtml.

23 "The United States and China agree that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors." See The White House Office of the Press Secretary. "Fact Sheet: President Xi Jinping's State Visit to the United States."Last Modified September 25, 2015.https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

24 "State and non-state actors should not conduct or knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace." See The Global Commission on the Stability of Cyberspace. "Global Commission proposes definition of the public core of the Internet."Last Modified July 5, 2018. https://cyberstability.org/news/global-commission-proposes-definition-of-the-public-core-of-the-internet/.

25 Dennis Broeders. The Public Core of the Internet: An International Agenda for Internet Governance. Amsterdam: Amsterdam University Press, 2015. 7.

26 See European Parliament. "REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)." Official Journal of the European Union, last modified April 17, 2019. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX-%3A32019R0881&qid=1623624957963.

27 See United Nations Office for Disarmament Affairs. "Open-ended Working Group."Accessed June 17, 2021. https://www.un.org/disarmament/open-ended-working-group/.

28 "States should not target ICT companies to insert vulnerabilities (backdoors) or take actions that would otherwise undermine public trust in products and services." See Microsoft. International Cybersecurity Norms: Reducing conflict in an Internet-dependent world. Microsoft Corporation, 2015.https://www.microsoft.com/en-us/download/confirmation.aspx?id=45031.

29 See Global Commission on the Stability of Cyberspace. "Norm to Avoid Tampering."Accessed June 17, 2021. https://cyberstability.org/norms/#toggle-id-3.

30 See China.org.cn. "Global Initiative on Data Security."Accessed June 17, 2021. http://www.china.org.cn/chinese/2020-09/15/content_76704524.htm.

31 "Not to use information and communications technologies and information and communications networks to interfere in the internal affairs of other States or with the aim of undermining their political, economic and social stability." See Ministry of Foreign Affairs of the People's Republic of China. "International Code of Conduct for Information Security."Accessed June 17, 2021. http://infogate.fmprc.gov.cn/web/ziliao_674904/tytj_674911/zcwj_674915/t858317.shtml.

32 See United Nations Human Rights Office of the High Commissioner. "International Covenant on Civil and Political Rights." Accessed June 17, 2021. https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.

33 See Global Commission on the Stability of Cyberspace. "Norm to Protect Electoral Infrastructure."Accessed June 17, 2021. https://cyberstability.org/norms/#toggle-id-2.

About the Author

Xu Peixi is Professor and Director of the Global Internet Governance Studies Center at the Communication University of China (CUC). He obtained his Doctoral Degree from CUC and a Licentiate Degree from the University of Tampere, Finland. His research interests include Global Communication, Internet Governance, and Cybersecurity. He has authored over 50 articles published in academic journals, including *China Information Security* and *Modern Communications*, as well as three books: Global Governance from Traditional Media to the Internet (Tsinghua University Press), The Shaping of Cyber Norms: Origins, Disputes, and Trends (China Social Sciences Academic Press), and Digital Cold War Studies (Guangming Daily Press). Xu Peixi is a member of the MAG of China IGF. He is an active participant of IGF and China-EU, China-U.S. cyber dialogues. He can be reached at xupeixi@gmail.com.

Cyberstability Paper Series

New Conditions and Constellations in Cyber

The Pro and Contra of an Incidents at Sea Agreement for Cyberspace

Contra

Benjamin Bahney
Senior Fellow, Lawrence Livermore National Laboratory's Center for Global Security Research (CGSR)
Jonathan Reiber
Senior Director for Cybersecurity Strategy and Policy, AttackIQ
Brandon Williams
Cybersecurity postdoctoral Fellow, Lawrence Livermore National Laboratory's Center for Global Security Research (CGSR)

Pro

Alexander Klimburg, PhD
Director, Global Commission on the Stability of Cyberspace Initiative and Secretariat

December 2021

Contra: The Incidents at Sea Agreement is a Poor Model for Cyberspace

Benjamin Bahney | Senior Fellow, Lawrence Livermore National Laboratory's Center for Global Security Research (CGSR)

Jonathan Reiber | Senior Director for Cybersecurity Strategy and Policy, AttackIQ

Brandon Williams | Cybersecurity postdoctoral Fellow,Lawrence Livermore National Laboratory's Center for Global Security Research (CGSR)

Tensions between the major powers have risen significantly in recent years, and cybersecurity matters have been some of the key flash points. The U.S. has long perceived that China has fueled its economy and military rise by stealing intellectual property, and the Russian government interfered in the 2016 U.S. elections using disinformation and influence operations in cyberspace. Conversely, Russia and China have expressed consternation about U.S. "left of launch" and Stuxnet-like capabilities that threaten their infrastructure and their strategic forces.[1,2] Reciprocal concerns have been widespread over quotidian hacking, interference, and in some cases destruction of private-sector data and systems.

U.S. Government responses to these challenges have run the gamut. U.S. policymakers have indicted foreign military operators for cybertheft, treating these incidents as traditional espionage, and analysts suspect that in other cases the U.S. has undertaken reciprocal responses where the behavior was more injurious.[3] But the policy community also seeks new diplomatic solutions. A 2014 bilateral agreement between Presidents Obama and Xi Jinping attempted to reduce cy-

Benjamin Bahney is a Senior Fellow at Lawrence Livermore National Laboratory's Center for Global Security Research (CGSR) where he studies strategic competition in the 21st century in the areas of space, cyber, and advanced science and technology.

Jonathan Reiber is Senior Director for Cybersecurity Strategy and Policy at AttackIQ, where he leads the company's narrative and content creation programs and directs key strategic issues. During the Obama administration he served as Speechwriter and Chief Strategy Officer for Cyber Policy in the Office of the Secretary of Defense

Dr. Brandon Kirk Williams is a cybersecurity postdoctoral fellow at the Center for Global Security Research at Lawrence Livermore National Laboratory. His research focuses on the intersection of cybersecurity, emerging technology, and national security policy.

bersecurity tensions by proscribing states conducting intellectual property theft in cyberspace for commercial gains, and by establishing new track 1.5 groups to work on cyberspace law enforcement and military stability issues. But tensions around cyberspace issues have only risen since 2014, and arms control proponents seek additional rules of the road and consultative mechanisms to build stronger adherence to international law and norms and to create new channels of engagement between militaries and diplomats.

In our analysis the idea of an INCSEA for cyberspace fails to be relevant to today's security environment on three key counts: it does not match the political conditions between the major powers, it does not fit the operational realities of the cyberspace domain, and it does not address the key policy challenges and stability challenges related to cybersecurity.

At first blush, a cyberspace agreement that emulates the 1972 incidents at sea (INCSEA) agreement—which built similar mechanisms for the high seas once the Soviets established a blue water Navy—seems like a plausible avenue toward stabilizing military cyberspace affairs. However, in our analysis the idea of an INCSEA for cyberspace fails to be relevant to today's security environment on three key counts: it does not match the political conditions between the major powers, it does not fit the operational realities of the cyberspace domain, and it does not address the key policy challenges and stability challenges related to cybersecurity. To make these points, first we will lay out the INCSEA agreement in historical context to understand the conditions leading to its promulgation and the problems it solved. Second, we will analyze the INCSEA concept in the face of the operational realties and policy problems in the cyberspace domain, and third we will discuss how it falls short of addressing the key problems of the cyberspace domain today.

The Agreement between the U.S. Government and the Government of the Russian Federation on the Prevention of Incidents On and Over the High Seas was signed on May 25, 1972, by Secretary of the Navy John Warner and the Soviet Union's Commander in Chief of the Navy Sergei Gorshkov. Commonly referred to as INCSEA, the bilateral agreement binds both parties to stated rules for the conduct of each country's ships and airplanes on and over the high seas to reduce the risk of escalation.[4]

INCSEA established a code of conduct for transparency, non-interference, information sharing, advanced notice of activity, and annual consultations, as well as an agreement to avoid threatening activity. INCSEA built on previous international agreements—such as the 1958 Geneva Convention of the High Seas—that codified rules for the operation of military and civilian vessels on and above the high seas. INCSEA does not restrain limits on force size, exercises, or the operation of each nation's navy or air force.

Representatives from the United States and Russia meet annually on a bilateral basis to reaffirm INCSEA and to discuss its application of ship-to-ship and air-to-air contact during the previous year. The consultations preserve INCSEA's continuity and place it in a suite of important bilateral confidence building measures originating in the relaxation of Cold War superpower tension in the early 1970s period of détente.

President Lyndon Johnson's administration exchanged the first diplomatic notes with the Soviet Union that ultimately culminated in INCSEA's 1972 signing at a high tide of superpower diplomacy. Informal bilateral discussions between the navies began in 1966, but a worrying crescendo of near

misses in 1968 convinced the Departments of State and Defense to amplify requests for a formal agreement. A TU-16 bomber, in one instance, crashed in May 1968 after buzzing U.S. ships operating in the Norwegian Sea, raising the risk of collisions that could spiral into escalation. Undersecretary of State Nicholas Katzenbach wrote Deputy Secretary of Defense Paul Nitze in 1968 warning him of the risks and an ostensible lack of interest from the Soviet Union. Overtures throughout 1968 from the U.S. Departments of State and Defense to Soviet counterparts went unanswered until the climate of superpower relations improved.[5]

Henry Kissinger notified Richard Nixon that the impasse broke in 1971 after Soviet diplomats formally requested consultations on incidents at sea. The president approved Kissinger's request to proceed with formal dialogue and consolidate the effort in the hands of the National Security Council in place of overlapping formal and private conversations.[6] "We seem to be enjoying something like an 'era of good feeling'," the United States' ambassador to Russia reported after productive deliberations between the two superpowers on incidents at sea. Forward progress on a future INCSEA occurred, however, only in the context of Détente's thaw.[7]

The Soviet Union and the United States signed INCSEA during a 1972 summit in Moscow when Nixon and Soviet Premier Leonid Brezhnev signed the Strategic Arms Limitation Treaty. In preparation for the state visit, Kissinger alerted Nixon that a raft of agreements on disparate subjects were slated for announcement: space, the environment, health, science and technology, commerce, and incidents at sea. Both parties formalized INCSEA amidst a rewiring of the frayed bilateral circuits to resume conversations on traditional state-to-state matters.[8]

INCSEA and the decades of annual consultations improved the condition of naval security and strategic stability for approximately fifty years. It ensured safety of navigation on and over the high seas even during instances of heightened tension, provided commanders with stated rules, created the bilateral machinery for dialogue, and reduced the opportunity for pilot or captain miscalculation. By the mid-1980s, troubling episodes on and above the high seas had declined markedly, and INCSEA served as evidence of a successful confidence-building measure.

The relationships between the three major cyberspace powers today—namely, the U.S., China and Russia—are far more contentious than what was present during the period of détente leading up to the INCSEA agreement.

INCSEA, ultimately, was a product of a specific historical moment when two competing powers mutually agreed to diminish the strategic, tactical, and accidental escalatory catalysts. Senior leaders in the United States and the Soviet Union recognized that competition could occur without risky conduct below the threshold of war. Confidence-building measures governing visible objects and domains, such as the high seas, proved easier to implement. Policymakers in Washington and Moscow mutually agreed that they benefited by reducing tension, and a transparent code of conduct on the high seas was one lever by which to restore stability for bilateral relations and geopolitics.

However, the political conditions that led to INCSEA are largely missing today. While there is a movement toward some agreement on normative measures in the United Nations, the required political conditions are much broader than that. The relationships between the three major cyberspace powers today—namely, the U.S., China and Russia—are far more contentious than what was present during the period of détente leading up to the INCSEA agreement. There is no common view between the powers on how cyberspace relates to strategic stability, which was a clear

precursor to INCSEA. There is also no clear motivation by the major powers to explore new arms control measures for cyberspace, and no shared drive to tamp down tensions as there was in the late 1960s and early 1970s after the U.S. and the Soviet Union had come close to the brink during the Cuban Missile Crisis in 1962.

Today's arms control environment, rather, is one where we see significant backsliding with major treaties having been recently jettisoned, such as the Anti-Ballistic missile treaty, the Intermediate Nuclear Forces Treaty, and the Open Skies Treaty. Rather than cooperation and threat reduction, the major powers appear to be in a mindset of unbridled competition—more akin to the 1950s and early 1960s when we saw significant international crises, and when arms control seemed far off into the future. But surely, political conditions could change in the wake of a major crisis, or given significant changes in the leadership of the major power states. So if these conditions do change, could INCSEA address the fundamental realities and challenges of cyberspace competition?

Not really. The reasons are three-fold.

First, cyberspace operations occur in cyberspace via a network of data centers, servers, routers, switches, computers, and devices owned by private and government entities in sovereign territory—and there is no similar consensus upon the existence of an equivalent of the "high seas" in cyberspace. Even if operators conceal their locations, they are always operating in sovereign territory on someone's network. Damage, disruption, or theft done to data on a network therefore impacts a specific data owner or operator, and is a violation of sovereignty.

Second, while cyberspace operators might "bump into" each other on the infrastructure if they are both present on a network—two intruders passing in the night, as it were—these are virtual interactions and seem unlikely to cause inadvertent material harm in the same way that navies could do so on the high seas. The intruder would need to manipulate data and cause material and irreversible harm for it to be analogous, in some way, to two ships colliding on the open seas. Similarly, there would need to be some risk that an incident of cyberspace operators bumping into each other could rise to the level of an armed attack under international law, via the irreversible destruction of life or property, if it were to plausibly carry a significant risk of escalating to war. This is an unlikely occurrence in cyberspace.

Third and most importantly, if the United States and Russia or China are to have productive conversations about cyberspace, the most important issue is for the states to make progress on adhering to bounds of acceptable state behavior in peacetime and conflict. This is a far greater legal and policy challenge for the bilateral relationship, and an INCSEA-like agreement is wholly irrelevant to its resolution.

Cyberspace is a new arena of operations. Over the last decade, as access has increased exponentially across the globe, adversaries have flourished in the "gray space" below the level of outright conflict that cyberspace affords, escalating their operations against the United States without fear of real retribution. That is how China has stolen U.S. intellectual property through cyberspace with impunity, why North Korea broke into and damaged Sony Pictures Entertainment's networks before the release of the parody film The Interview, and why the Russian Federation conducts cyber-enabled disinformation operations in advance of U.S. elections, penetrates U.S. critical infrastructure, and sows seeds of social discord within the U.S. population. For more than a decade, revisionist nation states have exploited the vulnerabilities that cyberspace affords. Countries have conducted hostile operations online, through disinformation and cyberspace operations, without

ever having to leave their home, with limited resource investments, recognizing that the United States was not entirely sure how best to respond.

For years the United States largely held back against each of the above actors, not wanting to trigger a tit-for-tat response in cyberspace that could escalate. Instead, the United States sought to impose retributive costs through indictments and sanctions. This did not help achieve deterrence in cyberspace. But perhaps the Russian government's interference in the 2016 U.S. Presidential election was a watershed moment. In 2018, the United States military gained the authority with which to conduct cyberspace operations to stop cyberattackers in advance of attacks against core U.S. interests, an expression of the new U.S. strategy to "defend forward" in cyberspace.[9] This suggests that, if the United States has indicators and warning of a potential cyberattack against its vital interests—such as its critical infrastructure—as it did in advance of the 2018 elections, the United States may take action to defend American interests online. Outside of the U.S. military's use of operations in cyberspace, following a spike in ransomware attacks in 2020 and 2021 against hospitals and infrastructure, the U.S. Department of Justice targeted cybercriminals by seizing their bitcoin holdings,[10] and the U.S. Treasury Department implemented sanctions on the global malware market by targeting cryptocurrency instruments.[11]

The goal of this increasingly forceful response posture is to help set and assert the bounds of acceptable behavior, along with deterring hostile activities, to include countries that allow ransomware operators to conduct criminal activities without fear of arrest. The Russian government's actions in the SolarWinds intrusion and in allowing ransomware groups to flourish within its borders remains a pre-eminent concern in matters of policy and law for the United States in cyberspace. This problem cannot be addressed through an INCSEA-like agreement because the principal issue is that the Russian government allows malicious cyberspace operators in its territory to act with impunity.

If there is any place for legal agreements in matters of cybersecurity, diplomacy should occur around the question of how to set and maintain responsible state behavior in cyberspace.

If there is any place for legal agreements in matters of cybersecurity, diplomacy should occur around the question of how to set and maintain responsible state behavior in cyberspace. The cybersecurity community has made progress here in multilateral fora. Concurrent with the United States increasing its efforts to deter and disrupt attacks on its interests, the United Nations countries have built on decades of work from the UN's cybersecurity Group of Governmental Experts (GGE) to affirm the need for norms of operations in cyberspace, such as refraining from targeting medical devices or other critical infrastructure.[12] But unlike with INCSEA, these multilateral agreements do not seem to have curtailed Russian malign influence operations in cyberspace.

Bilaterally, the U.S. and Russia put in place emergency communications during the Obama administration to tamp down the chance of conflict spiraling out of control. Increasing communication about strategic capabilities is certainly to the good, and that might be what has urged the call for an INCSEA-like treaty: to discuss and shape how forces operate. But the United States can pursue those discussions through existing lines of communication around norms and crisis management.

The analogies of an INCSEA treaty otherwise fail to demand a new direction for U.S. policy and law. Recall that the original INCSEA treaty established rules of the road for maneuvering military weapon platforms (and later, merchant marine ships as well) to include the use of flag communications between vessels. At times these frightening close maritime engagements involved nuclear

weapon platforms such as strategic missile submarines and bombers. INCSEA also set rules of the road for the use of weapon engagement threats such as the opening of bomb bay doors on bombers that are nearby ships, the use of fire control radars against other vehicles or vessels, and simulated attacks.

For these two conditions, there is clearly no analogue yet in cyberspace. There is no record of threatening engagements between military cyberspace operators of one country and the strategic platforms or weapon systems of another, nor do we know of equivalent "dangerous maneuvers" in cyberspace that could put either side at risk. Last, there is no clear way to brandish weapons threats from cyberspace operators against specific weapons systems or platforms. Cyberspace operators do not seem to saddle up to one another and show off their malware in a chat room to threaten the other side. The absence of these conditions makes it unlikely today that cyberspace operations could result in inadvertent nuclear escalation, or that cyberspace operators could scare strategic weapons operators and their chain of command into using their weapons.

For these reasons, it is doubtful that an INCSEA-like agreement for cyberspace would be germane to the security concerns of today's cyberspace competition, that it could tamp down strategic tensions between states, or that such an agreement could be practicable.

The INCSEA treaty of 1972 was clearly a product of a period when the major powers sought détente and a reduction in tensions, and incidents on the high seas—outside of sovereign waters—between military combatants in peacetime were a potential vehicle to accidental or inadvertent escalation between nuclear armed states. There is no relevant mapping of this historical context to the political situation in 2021, nor does the situation in maritime affairs in the late 1960s and early 1970s have any relevance to cyberspace operations today. While the political conditions for such agreements could change rapidly given a change in geopolitics, it is hard to imagine how the strategic and operational context of military competition in cyberspace could approximate the maritime context of the period.

The views and opinions of the authors expressed herein do not necessarily state or reflect those of the United States government or Lawrence Livermore National Security, Inc. LLNL-JRNL-829171

Endnotes

1 Kenneth Lieberthal and Peter W. Singer, "Cybersecurity and U.S.-China Relations," Brookings Institution, February 2012. https://www.brookings.edu/wp-content/uploads/2016/06/0223_cybersecurity_china_us_lieberthal_singer_pdf_english.pdf

2 Vladamir Radyuhin, "Stuxnet could have created Chernobyls: Russia," The Hindu, January 27, 2011. https://www.thehindu.com/news/international/Stuxnet-could-have-created-Chernobyls-Russia/article15535416.ece

3 Julien Barnes, "U.S. Begins First Cyberoperation Against Russia Aimed at Protecting Elections," New York Times, Oct 23, 2018. https://www.nytimes.com/2018/10/23/us/politics/russian-hacking-usa-cyber-command.html

4 "Agreement Between the Government of The United States of America and the Government of The Union of Soviet Socialist Republics on the Prevention of Incidents On and Over the High Seas," conclusion date: May 25, 1972, U.S. Department of State, https://2009-2017.state.gov/t/isn/4791.htm .

5 Nicholas Katzenbach, "Letter From the Under Secretary of State (Katzenbach) to the Deputy Secretary of Defense (Nitze)," Foreign Relations of the United States (FRUS), 1964-1968, Volume XIV, Soviet Union, Document 284, August 16, 1968. https://history.state.gov/historicaldocuments/frus1964-68v14/d284

6 Henry Kissinger, "Memorandum From the President's Assistant for National Security Affairs (Kissinger) to President Nixon," FRUS, 1969-1976, Volume XIII, Soviet Union, Document 113, February 16, 1971. https://history.state.gov/historicaldocuments/frus1969-76v13/d113

7 U.S. Embassy in the Soviet Union, "Telegram From the Embassy in the Soviet Union to the Department of State," FRUS, 1969-1976, Volume XIV, Soviet Union, Document 7, October 22, 1971. https://history.state.gov/historicaldocuments/frus1969-76v14/d7

8 Henry Kissinger, "Memorandum From the President's Assistant for National Security Affairs (Kissinger) to President Nixon," FRUS, 1969-1976, Volume XIV, Soviet Union, Document 227, May 15, 1972. https://history.state.gov/historicaldocuments/frus1969-76v14/d227

9 US CYBERCOM, "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command," US CYBERCOM website, April 2018. https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf

10 U.S. Department of Justice, "Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside," U.S. Department of Justice, June 7, 2021, available at https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside.

11 U.S. Department of the Treasury, "Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group," U.S. Department of the Treasury Office of Public Affairs, March 2, 2021, available at https://home.treasury.gov/news/press-releases/sm924

12 Josh Gold, "Unexpectedly, All UN Countries Agreed on a Cybersecurity Report. So What?," CFR Blog, March 2021, https://www.cfr.org/blog/unexpectedly-all-un-countries-agreed-cybersecurity-report-so-what

About the Authors

Benjamin Bahney is a Senior Fellow at Lawrence Livermore National Laboratory's Center for Global Security Research (CGSR) where he studies strategic competition in the 21st century in the areas of space, cyber, and advanced science and technology. His research is focused on how these new areas of competition alter strategic stability, deterrence, and escalation management. Also as the laboratory's Space Program leader, he oversees all work on both space science and space security. Ben has written for Foreign Affairs magazine, Foreign Policy, Lawfare, War on the Rocks, and has contributed to the opinion pages of the New York Times. Ben was a contributor to the U.S. Cyberspace Solarium Commission, particularly on public private partnerships. He was also a contributor to the edited volume Cross-Domain Deterrence: Strategy in an Era of Complexity published by Oxford University Press (2019). Ben was formerly an analyst at the RAND Corporation.

Jonathan Reiber is Senior Director for Cybersecurity Strategy and Policy at AttackIQ, where he leads the company's narrative and content creation programs and directs key strategic issues. During the Obama administration he served as Speechwriter and Chief Strategy Officer for Cyber Policy in the Office of the Secretary of Defense, where he authored the first two national cyberdefense strategies of the United States. His commentary has appeared in TIME Magazine, Foreign Policy, Lawfare, and The Atlantic Monthly and his research has been supported by the Smith Richardson Foundation, Watson Foundation, and Berkeley's Center for Long-Term Cybersecurity. He is the author of A Public, Private War, the findings of which were adopted by the U.S. Cybersecurity Solarium Commission and the National Defense Authorization Act of 2021. He is a graduate of Middlebury College and The Fletcher School.

Dr. Brandon Kirk Williams is a cybersecurity postdoctoral fellow at the Center for Global Security Research at Lawrence Livermore National Laboratory. His research focuses on the intersection of cybersecurity, emerging technology, and national security policy. His work addresses geopolitical competition and alliances in the Indo-Pacific and has been published in Lawfare and CGSR reports on Indo-Pacific Cybersecurity, strategy and emerging technology, and strategic competition with China. He earned a PhD in history from the University of California, Berkeley, where he completed a dissertation examining national security history that was supported by a Fulbright-Hays Grant for research in Indonesia.

Pro: Transposing the Incidents at Sea Agreement – A Thought Experiment

Alexander Klimburg, PhD* | Director, Global Commission on the Stability of Cyberspace and Secretariat

A lack of agreed signaling protocols nearly led to World War Three. On October 27, 1962, at the height of the Cuban Missile Crisis, the US Navy cornered one of the few Soviet submarines unaccounted for off the coast of Cuba. In an effort to convince the FOXTROTT-class sub B-59 to surface, the destroyer USS Cony employed practice depth charges—which, however, were not accurately identified as such by the beleaguered crew. When the sub did indeed surface and engaged in communication, an anti-submarine aircraft flew low over the sub and dropped flares and pyrotechnics. This convinced the captain of the sub to crash drive, and, according to the detailed account in the 2020 book *Nuclear Folly,* a vigorous debate ensued on board the ship as to whether this constituted an attack, and the order was given to fire the sub's nuclear torpedoes, each with 10 Kiloton warheads, at the US navy task force. It was only in the last moment that the fire order was rescinded.

The 1972 Incident at Sea Agreement (INCSEA) was a milestone in de-escalation and confidence building. In clear and concise language, it created rules for a number of possible scenarios where Soviet and American navy forces might meet on the high seas—such as that which occurred during the Cuban Missile Crisis, where misunderstandings over signaling nearly led to an apocalypse. The success of INCSEA did not come lightly. By the time it was signed, ten years after the

* For the pro/contra article series the author reclused himself from his role as editor and reviewer of the Cyber Stability Paper series, and did not see the opposing article in advance.

Alexander Klimburg is the Director of the Global Commission on the Stability of Cyberspace Initiative and Secretariat, and the Director of the Cyber Policy and Resilience Program at The Hague Centre for Strategic Studies. He is also a Senior Associate at the Center for Strategic and International Studies (CSIS) and an Associate Fellow at the Austrian Institute of European and Security Policy.

incident described above, the rapidly expanding Soviet and US Navies were increasingly bumping into each other—often enough literally. The potential for "inadvertent escalation"—i.e., accidental war—was obvious. Agreed-upon norms were clearly needed. However, it still took both sides nearly four years to negotiate the agreement after the US first proposed it. But it was worth it; although the Cold War would go on to thaw and freeze and thaw again, the military-to-military agreements held sound, and prevented something worse from happening. In 1983, Secretary of the Navy John Lehman cited the accord as "a good example of functional navy-to-navy process" and credited this area of Soviet-American relations with "getting better rather than worse." In 1985, he observed that the frequency of incidents was "way down from what it was in the 1960s and early 1970s." This was despite a much-expanded navy on both sides.

The success of INCSEA has often been remarked upon when considering possible agreements in dealing with escalating cyber tensions today—after all, "disentangling" forces in cyberspace may seem like a practical and useful step in order to avoid serious accidents. Indeed, if anything, the scope of misunderstandings in cyberspace is even larger then that between navies during the Cuban Missile Crises: the realities of the domain mean that, for instance, it can be difficult for a cyber defender to differentiate between a malicious act as an attempt at espionage or as preparation for an act of war. INCSEA is not the only such agreement from which to draw, and the 1989 Prevention of Dangerous Military Activities Agreement[2] has some very promising cyber-adaptable aspects as well, as we shall see later.

But INCSEA is often evoked as the main model for a potential operational cyber agreement.[3] Detractors to the INCSEA-for-cyber (INCSEA-C) model sometimes like to point out that sea and cyber domains are not mirror images of each other. This is true, but the differences should not be overemphasized. All domains are unique, and it is the commonalties that need to be considered in a transposition, not the differences. The challenge, for instance, of establishing definitive attribution also exists at sea, and both planes and especially submarines are not always clearly identifiable.[4] And, as with navy forces, cyber forces have to "navigate" a domain that is often not bound by territorial sovereignty, and must consider civilian traffic as well.

The position of the United States (and most of the like-minded group of liberal democracies) over the last decade has been to avoid any formal political agreement on cyber conflict, for at least four good reasons: Firstly, most potential terms in cyber "treaties" were considered to be unverifiable, and would lead only to rampant cheating (or the expectations of such) and thus would prompt even more instability. Secondly, the implication that current International Law was not sufficient would create a precedent to open up other areas to new negotiation. Thirdly, any treaties on cyberspace would imply that states were the ultimate arbiter of the entire domain, conflicting with the Western position of a nonstate-led Internet. Fourthly, Russia has persistently led China and others in trying to equate what they view as psychological information warfare with technical cyberattacks. Effectively, this has amounted to focusing on means to protect what they call their "Internet segment" from content they consider destabilizing. When in September 2020 Russia's President Putin offered to negotiate with the United States on INCSEA-for-cyber,[5] these four points were clearly apparent, and he added a fifth reason to refuse such an offer: not giving Russia the status of a peer with the United Sates in a bilateral agreement, something undeniably politically important to Vladimir Putin. As a result, the Russian INCSEA-C offer was largely and understandably dismissed by US and Western commentators.[6]

Even though the INCSEA-for-cyber as a bilateral US–Russian agreement may be out of the question for the moment, there are good reasons why an INCSEA-C could be considered in a differ

ent, multilateral format, although not on the basis of the Russian September 2020 proposal. For instance, it could be considered as a new Confidence Building Measure within the Organization of Security and Cooperation in Europe (OSCE, although China would be absent), or even as a Memorandum of Understanding appended to existing UN First Committee initiatives. For the four basic reasons that like-minded democracies tend to (rightly) refuse cyber agreements do not apply here: "disentangling cyber" does not require counting cyber forces or even clear attribution of actual "attacks," so the first concern of cheating leading to escalation is largely mute. If cast as an agreement (let alone as a Confidence Building Measure or Memorandum of Understanding), it would not be a "treaty" in that it would create new international law,[7] but quite the opposite (as we shall see below), it can reinforce existing law—so the second concern would be mute. Regarding the third concern on undermining the nonstate-led Internet governance model: the focus is only on proscribing state behavior, so with correct wording this danger could be avoided as well. And regarding the fourth concern—not equating psychological-effect actions such as propaganda and covert influencing with the use of force and armed attack—this has been a cornerstone of international law for decades, and should not be reversed, despite recent Western military's considerations of responding to disinformation with kinetic-equivalent operations as a counter measure under international law. This precondition admittedly would likely be the largest stumbling block in getting the process off the ground.

Even though the INCSEA-for-cyber as a bilateral US–Russian agreement may be out of the question for the moment, there are good reasons why an INCSEA-C could be considered in a different, multilateral format, although not on the basis of the Russian September 2020 proposal.

But if all this were possible, that would leave the final, perhaps most important, question: what would an INCSEA-for-cyber actually do? What would it look like? This is where the efficacy of the original INCSEA agreement comes into play, where the military negotiators crafted a bare-bones agreement on three pages and with five articles of agreement.[8] As a thought experiment, it is an interesting challenge to transpose the document directly to cyber, although, immediately, some transpositions are easier than others.

For instance, Article I of the INCSEA would already seem a stumbling block. In the original document, definitions of "ship," "aircraft," and "formations" are agreed upon—and only in 122 words. This would undoubtedly be trickier for INCSEA-C; while the Internet, computers and networks might be easy to define, the stumbling block cyber/information/data "weapon" could be huge. The solution? Do not refer to weapons, but rather to possible effects (such as "interfering with..") that are technologically independent. A similar track has been taken with the current norms of restraint put forward in the UN First Committee processes.

Article II of INCSEA directly references and invokes the "International Regulations for Preventing Collisions at Sea" (later called COLREGs), a set of agreements under the International Maritime Organization that are commonly referred to in the document as "Rules of the Road." Veteran watchers of the UN First Committee Processes will remember that the eleven norms agreed upon in the 4th Group of Governmental Experts (GGE) Report[9] are often described as "rules of the road." In both cases, the intent was to reinforce existing international law while explicitly spelling out nonbinding and voluntary norms of behavior. The same principle could apply for Article 2 in an INCSEA-C: a clear commitment to the UN General Assembly-endorsed eleven norms would

provide both a common point of departure while reinforce existing international law. Just like the COLREGs outlined in 1972, the eleven GGE norms would represent a "common language" on specific behavior that is partially only further spelled out in the INCSEA-C. The importance of this common baseline is critical; one criticism of a similar bilateral military agreement between China and the United States is that it has largely failed due to a lack of common rules of the road being spelled out.[10]

Article III of INCSEA focuses on "hazardous actions and maneuvers," and a number of ideas are remarkably pertinent for a transposition to cyber. For instance, Article III paragraph 6 directly says that the Parties should "not simulate attacks," by aiming guns or such, at each other. One of the most significant challenges in cyber is that some activities do not seem to have other functions (such as intelligence gathering) and are either a clear threat of the use of force, or even a case of advanced preparation of the battlefield. For instance, leave-behinds (large encrypted files) in critical infrastructure networks without any meaningful raw intelligence value can often only be interpreted as a preparation for attack. Often enough, activities observed, e.g., in the power grid meet this case, and sometimes the attacker may even draw attention to their existence by a cyber "shot across the bow" that may be excessively escalatory. In the same paragraph 6, another interesting parallel can be found, namely "not using searchlights or other powerful illumination devices to illuminate the navigation of bridges of passing ships." The reason for this is obviously one of blinding the crew and thus imperiling ship navigation. A near parallel for this could actually be "excessive" or malicious port and network scanning activities. While port and network scanning are regular and should be considered part of the background noise of the Internet, excessive or malicious port scanning, such as shining a blinding light into a ship's pilot's eyes, can cause a defender undue concern that a serious attack is coming. It can even directly affect some network activity. Speaking of affecting network activity, paragraph 3 explicitly excludes navy ships from conducting maneuvers through areas of heavy traffic. Something similar could be said about an injunction of governments prohibiting the conducting of training (or offensive peacetime operations) that unduly infringes upon the availability or integrity of civilian services.

Often enough, activities observed, e.g., in the power grid meet this case, and sometimes the attacker may even draw attention to their existence by a cyber "shot across the bow" that may be excessively escalatory.

One of the most intriguing parallels to be drawn in Article III is, however, paragraph 4. It reads "ships engaged in surveillance of other ships…avoid executing maneuvers embarrassing or endangering the ships under surveillance."[11] In seaman's terms, "embarrassing another ship" means causing it to take evasive actions in a way that may endanger it or others. There is a case to be made that there is such a thing as "cyber embarrassment": a case where the surveilling actor causes the defending actor to undertake actions damaging to itself or others. If, for instance, a cyber espionage case is so severe that, e.g., a foreign ministry is forced to disconnect itself from the Internet to attempt to clean up the attack, this "cyber maneuver" would cause significant follow-on effects, such as, for instance, citizens in urgent need of help would not be able to contact their representatives. This example is made even more poignant in purely civilian cases, such as when emergency or 911 numbers and similar numbers are affected. This author has speculated on what cases of cyber-espionage could potentially rise to the level of a threat or the actuality of use-of-force,[12] and more recently law scholars have also started to opine on the matter.[13] The notion of a "cyber embarrassment" is therefore a potentially rich field for deliberation that easily exceeds this short essay.

Article IV of INCSEA concentrates on the hazardous maneuvering of aircraft over ships. But it provides a useful point of departure for a cyber version to concentrate on something similarly connected to one domain but part of another—and that is security of communication links, in particular those of undersea cables and satellite. While nations have always considered spying on communication cables (and satellites) to be a justified activity in peacetime, some limitations may be reasonable if there is a reasonable chance that the availability or integrity of civilian services could be affected. This would include any kind of interference that interrupts the communication completely, such as, for instance, by inadvertently cutting a cable while tapping it, or a poorly-designed cyber espionage attack on a satellite or ground station that renders the system temporarily inoperable. While these infrastructures are already indirectly covered in international law as well as the 4th and 6th UN GGE Report, they have not been previously explicitly mentioned. This would also be a great opportunity to directly address the security of the global undersea cable infrastructure overall, also highlighting that implied conventional threats carried out with loitering with naval vessels (as occurred in 2015, 2018, and recently in 2021[14]) would be out of bounds as well. Artful wording in this paragraph would even be able to address yet another increasingly problematic issue, namely, one of wideband GPS jamming, which has led to a number of naval incidents as of late.[15] Ideally, a separate Article could even be considered binding all parties to non-interference in the availability of integrity of the basic backbone infrastructure of the global Internet. A norm proposed by the Global Commission on the Stability of Cyberspace (GCSC) on the non-interference with this so-called "public core" could provide a baseline; indeed, much of the spirit of the GCSC's work was already adopted in the reports of the 2021 Open-Ended Working Group and GGE.

There is a case to be made that there is such a thing as "cyber embarrassment": a case where the surveilling actor causes the defending actor to undertake actions damaging to itself or others.

This Article could also allow the introduction of a category of protection found in a different mil-mil agreement, namely the "Special Caution Areas" (SCAs) mentioned in the 1991 Prevention of Dangerous Military Activities Agreement.[16] SCAs are defined by each party in mutual agreement, and have special protective measures assigned to them. For instance, an SCA could include the dedicated nuclear command and control infrastructure of a country,[17] and the activity in question could be a prohibition on all kinds of cyber activity in this SCA to avoid any appearances that these capabilities were to be preemptively eliminated. SCAs could also, however, include a number of civilian infrastructures, including large Internet Exchange Points and others. Indeed, the aforementioned "public core of the Internet" infrastructure would represent an easy SCA to which all could likely agree.

The remaining Articles address the exchange of information, both operationally at sea as well as strategically, between military staffs reviewing the agreement. In cyber terms there have been repeat efforts to instigate similar communication protocols, both at the operational and political (but not at the in-between strategic) levels, but they often have been inconclusive. The most common operational approach has been to identify national technical points of contact[18] on the defender side (national CERTs or equivalent). Most of these arrangements (with notable exceptions such as CBM 8 of the OSCE[19]) miss a crucial element: an escalation ladder in case of non-responsiveness, going up to the political level, such as, for example, to a responsible cabinet minister, if necessary.[20] Further, there are few (if any) such regular strategic exchanges between actual cyber commands or similar entities that are responsible for offensive cyber operations. A "cyberhotline" can be described as a political level tool, and, if used without support from regular links established on the

strategic level, can potentially be a dead end, as seen in the 2016 US Presidential Election.[21] Equally important, therefore, are multiple direct international links between leading officials and officers in cyber policy. Finally, there is no process yet within the multilateral space by which to have a closed emergency consultation on cyber issues—there is no "in between" forum between a closed emergency UN Security Council meeting and bilateral or public exchanges, such as the confidential network the OSCE tries to provide to its participating states.[22] This means that there is a lack of options by which states may properly signal to each other that there is a crises, potentially leading to a state of public re-criminations and loss of escalation control.

Overall, the success and failure of such an agreement would largely depend on the sophistication of those negotiating it, and it would require some time, until the political will has been adequately mobilized.

In conclusion, it may need to be stressed that any good agreement would require sacrifices on both sides. There are points in the above thought-experiment that might be difficult for members of the like-minded group of liberal democracies to accept, and there are certainly points that would be difficult for Russia and China to accept as well. It will only be feasible if those responsible think that such an agreement will have more benefits then costs—and it is very obvious that costs and benefits (the equites) are not being assessed equally across and between governments. The situation is further complicated by the reality that the two main ideological blocks in cyber have fundamentally different priorities in what they want from these discussions—the United States and the like-minded group may be worried about "cyber war," but Russia and China are certainly more concerned with what they think is "Information war."[23] The INCSEA-C thought experiment is clearly orientated toward the former concern. Overall, the success and failure of such an agreement would largely depend on the sophistication of those negotiating it, and it would require some time, until the political will has been adequately mobilized. However, as we have seen over recent years, the political will and intent on cyber issues has gyrated widely, often depending on serious cyber incidents to set the agenda. Smart policy making will be aware of the threat of allowing the news headlines to dictate the conversation, and would be well advised not only to react, but to get ahead of the curve. Thinking seriously about a multilateral Incident at Sea for the Cyber model is a good step in regaining the initiative.

Endnotes

1 "Agreement Between the Government of The United States of America and the Government of The Union of Soviet Socialist Republics on the Prevention of Incidents On and Over the High Seas," conclusion date: May 25, 1972, U.S. Department of State, https://2009-2017.state.gov-/t/isn/4791.htm

2 "Prevention of Dangerous Military Activities Agreement," WikiSource, last modified July 16, 2019, https://en.wikisource.org/wiki/Prevention_of_Dangerous_Military_Activities_Agreement.

3 This includes also by representatives of the United States State Department.

4 Attribution is remarkably similar in places—when claiming infringements of an air defense identification zone, common practice of states was not to require technical evidence (such as radar pictures)—for the same reasons that attribution of cyber attacks are often done without presenting technical data.

5 Tom Balmforth and Anton Kolodyazhnyy, "Putin says Russia and U.S. should agree not to meddle in each other's elections," Reuters, September 25, 2020, https://www.reuters.com/article/uk-russia-usa-putin-idUKKCN26G1OM

6 For instance, see Greg Austin and Alexander Stronell, "Why Putin's call for a US–Russia cyber reset will fall on deaf ears," The International Institute for Strategic Studies, October 1, 2020, https://www.iiss.org/blogs/analysis/2020/09/csfc-putins-cyber-reset. However, it needs to be pointed out that a former senior US Department of State representative stated that he and his colleagues had raised the idea of the INCSEA-C themselves in a multilateral context before, and the US government overall has been open to this idea in the past.

7 The majority view of scholars is that the original INCSEA is still considered as an "agreement," not a "treaty"—while the signing parties clearly define it as an agreement (e.g., not creating international law, and not requiring ratification by the US Senate), this might change with time, as other states adapt it as common practice.

8 See Takuya Shimodaira, "Chapter 7. Measures to Enhance Maritime Safety—Expansion of Code for Unplanned Encounters at Sea (CUES) Exercise," International Symposium on Security Affairs 2017 by the National Institute for Defense Studies (July 2017), http://www.nids.mod.go.jp/english/event/symposium/pdf/2017/e-07.pdf

9 United Nations Group of Governmental Experts, "Group of Governmental Experts on Developments in the
Field of Information and Telecommunications in the Context of International Security," United Nations, July 22, 2015, https://undocs.org/A/70/174

10 This is the Military Maritime Consultative Agreement (MMCA) of 1998. For a critique, see Shimodaira, "Chapter 7. Measures to Enhance Maritime Safety", http://www.nids.mod.go.jp/english/event/symposium/pdf/2017/e-07.pdf

11 "Agreement Between the Government of The United States of America and the Government of The Union of Soviet Socialist Republics on the Prevention of Incidents On and Over the High Seas," Article III, paragraph 4.

12 Alexander Klimburg, The Darkening Web: The War for Cyberspace, (New York: Penguin Books, 2017).

13 Duncan B. Hollis and Tsvetelina van Benthem, "What Would Happen If States Started Looking at Cyber Operations as a 'Threat' to Use Force?," Lawfare, March 30, 2021, https://www.lawfareblog.com/what-would-happen-if-states-started-looking-cyber-operations-threat-use-force

14 H. I. Sutton, "Russian Spy Ship Yantar Loitering Near Trans-Atlantic Internet Cables," Naval News, August 19, 2021, https://www.navalnews.com/naval-news/2021/08/russian-spy-ship-yan-

tar-loitering-near-trans-atlantic-internet-cables/ and "Concern over Russian ships lurking around vital undersea cables," CBS News, March 30, 2018, https://www.cbsnews.com/news/russian-ships-undersea-cables-concern-vladimir-putin-yantar-ship/

15 Gareth Corfield, "Russia spoofed AIS data to fake British warship's course days before Crimea guns showdown," The Register, June 14, 2021, https://www.theregister.com/2021/06/24/russia_ais_spoofing/

16 "Prevention of Dangerous Military Activities Agreement," WikiSource, https://en.wikisource.org/wiki/Prevention_of_Dangerous_Military_Activities_Agreement

17 This is notwithstanding some claims by US analysts that some nuclear powers may have "purposely entangled" their conventional and nuclear C&C structure to prevent them from being targeted. Even if true, it is irrelevant—using the example of the DMAA, an SCA may only be agreed by all parties, not declared unilaterally.

18 One of these is the MERIDIAN Group Contact List, although this does include China and Russia.

19 Organization for Security and Co-operation in Europe Permanent Council, "Decision No. 1202 OSCE Confidence-Building Measures To Reduce The Risks Of Conflict Stemming From The Use Of Information And Communication Technologies," Organization for Security and Co-operation in Europe, March 10, 2016, https://www.osce.org/files/f/documents/d/a/227281.pdf

20 A similar "contact escalation ladder" is implied in Confidence Building Measure 2 of the OSCE list. See, Organization for Security and Co-operation in Europe Permanent Council, "Decision No. 1202 OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies,".. This author proposed that component in the OSCE 1039 working group, and justified it with the experience of the China–Japan–Korea Memorandum of Understanding that utilized this approach.

21 The US–Russia "cyber hotline" was set up in 2013 on the basis of the famous nuclear "hot line," but was only used once, in 2016, to little effect. Erin Banco and Kevin Poulsen, "This Hotline Could Keep the U.S. and Russia From Cyberwar," The Daily Beast, March 07, 2019, https://www.thedailybeast.com/this-hotline-could-keep-the-us-and-russia-from-cyber-war

22 The OSCE Network is a secure, closed network that can send messages bilaterally but also to groups. Thomas Greminger, "Vienna Cyber Security Week—Protecting Critical Infrastructure—Opening remarks," Organization for Security and Co-Operation in Europe, March 11, 2019, https://www.osce.org/files/f/documents/9/7/415007.pdf

23 Alexander Klimburg, The Darkening Web: The War for Cyberspace, (New York: Penguin Books, 2017)

About the Author

Dr. Alexander Klimburg is Director of the Global Commission on the Stability of Cyberspace Initiative and Secretariat and Director of the Cyber Policy and Resilience Program at The Hague Centre for Strategic Studies. He is an Affiliate and former Fellow at Harvard University, and an associate fellow at the Austrian Institute of European and Security Policy. Alexander Klimburg has worked on numerous topics within the wider field of international cybersecurity. He has acted as an adviser to a number of governments and international organizations on national cybersecurity strategies, international norms of behavior in cyberspace and cyber-conflict (including war, cyber-crime, and cyber-espionage), critical infrastructure protection, and internet governance. He has participated in international and intergovernmental discussions within the European Union and the Organization for Security and Co-operation in Europe and has been a member of various national, international, NATO, and EU policy and working groups. He has given dozens of invited talks and regularly participates and organizes track 1.5 diplomatic initiatives as well as technical research groups. He is author and editor of numerous books, research papers, and commentaries and has often been featured in the international media, including in Newsweek, Reuters, and others. His most recent book The Darkening Web: The War for Cyberspace was published by Penguin Press.

Cyberstability Paper Series
New Conditions and Constellations in Cyber

This publication may be cited as:
Alexander Klimburg (Ed.), New Conditions and Constellations in Cyber, The Hague Centre for Strategic Studies, The Hague 2021.

ISBN: 9789492102874

Co-editor: Louk Faesen
Reviewers: Alexander Klimburg, Louk Faesen, Tim Sweijs, Frank Bekkers

The Hague Centre for Strategic Studies

HCSS helps governments, non-governmental organizations and the private sector to understand the fast-changing environment and seeks to anticipate the challenges of the future with practical policy solutions and advice.

The Hague Centre for Strategic Studies
Secretariat of the Global Commission on the Stability of Cyberspace
info@hcss.nl hcss.nl
Lange Voorhout 1
2514EA The Hague
The Netherlands

Cyberstability Paper Series

New Conditions and Constellations in Cyber