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

December 2021

Cyberstability Paper Series
New Conditions and Constellations in Cyber

Prioritizing Capacity Building as a Foundation for Cybersecurity and Stability

Christopher Painter | President of the Global Forum on Cyber Expertise

December 2021

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.

The opinions expressed in this publication are those solely of the author(s) and do not reflect the views of the Global Commission on the Stability of Cyberspace (GCSC), its partners, or The Hague Centre for Strategic Studies (HCSS).

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 other 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 embed 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.

About the Cyberstability Paper Series

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 are released on a rolling basis from July until December 2021, culminating in an edited volume. All papers will be available for open access, and a limited number of printed hardback copies are available.

Published by

GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

The Hague Centre
for Strategic Studies

The opinions expressed in this publication are those solely of the author(s) and do not reflect the views of the Global Commission on the Stability of Cyberspace (GCSC), its partners, or The Hague Centre for Strategic Studies (HCSS).