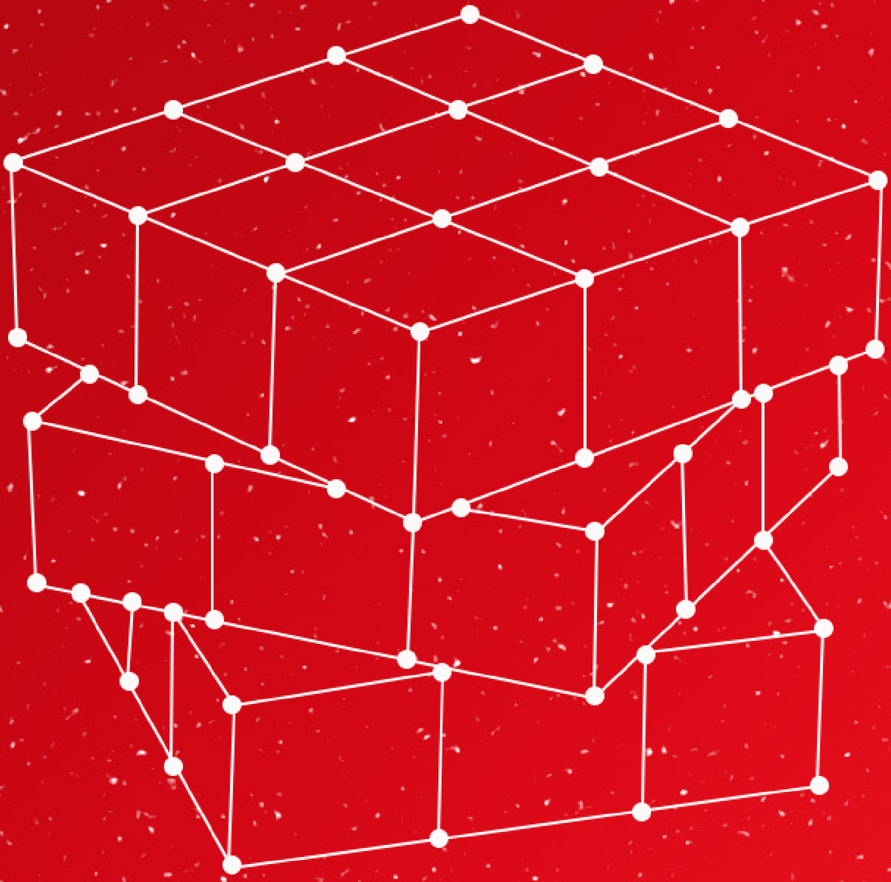
Cyberstability Paper Series
New Conditions and Constellations in Cyber

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)

December 2021



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)

December 2021

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 cyberattack 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.

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).

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 "public 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 presented 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 Cyberspace "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 Democracy.com? Governance in a Networked World, ed Elaine Ciulla Kamarck and Joseph S. Nye, Jr. (Mer-

rimack, 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).

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).