GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

TOWARDS A HOLISTIC APPROACH FOR INTERNET RELATED PUBLIC POLICY MAKING

CAN THE HELSINKI PROCESS OF THE 1970S BE A SOURCE OF INSPIRATION TO ENHANCE STABILITY IN CYBERSPACE?

Wolfgang Kleinwächter, Professor Emeritus from the University of Aarhus,
Former Director on the ICANN Board

GCSC **THOUGHT PIECE**
JANUARY 2018

GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

PROMOTING STABILITY IN CYBERSPACE TO BUILD PEACE AND PROSPERITY

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

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

The GCSC does not specifically endorse the respective publications, nor does it necessarily ascribe to the findings or conclusions. All comments on the content of the publications should be directed to the respective authors.

The Hague Centre for Strategic Studies

Lange Voorhout 1
2514 EA The Hague
The Netherlands

info@hcss.nl
HCSS.NL

EastWest Institute (EWI)

www.eastwest.ngo
communications@eastwest.ngo

ABOUT THE GLOBAL COMMISSION ON THE STABILITY OF CYBERSPACE

The Global Commission on the Stability of Cyberspace (GCSC) helps to develop norms and policies that advance the international security and stability of cyberspace. It promotes mutual awareness and understanding among the various cyberspace communities working on issues related to international cybersecurity. By finding ways to link the various intergovernmental dialogues on international security with the new communities created by cyberspace, the GCSC fulfils a critical need: supporting policy and norms coherence related to the security and stability in and of cyberspace by applying a multi-stakeholder approach to its deliberations on peace and security.

Chaired by Marina Kaljurand, and Co-Chaired by Michael Chertoff and Latha Reddy, the Commission comprises 26 prominent Commissioners representing a wide range of geographic regions as well as government, industry, technical and civil society stakeholders with legitimacy to speak on different aspects of cyberspace.

The GCSC Secretariat is provided by *The Hague* Centre for Strategic Studies and supported by the EastWest Institute.

ABOUT THE AUTHOR

Wolfgang Kleinwächter is a Professor Emeritus from the University of Aarhus where he was teaching a master course on Internet Policy and Regulation from 1997-2015. He was a Director on the ICANN Board (2013-2015) and a Special Ambassador of the NETMundial Initiative (2014-2016).

He is active in the field of transborder data flow and Internet governance since the 1980s. He was involved in the making of ICANN and has participated in various capacities in more than 50 ICANN meetings. He served six years in the NomCom (2009/2010 as its chair) and two years in the GNSO Council (2011-2013), elected by the Non-Commercial Stakeholder Group (NCSG), where he is a member of the NCUC. In the WSIS context he was appointed by UN Secretary General Kofi Annan as a member of the UN Working Group on Internet Governance (2003-2005) and served as Special Adviser to Nitin Desai, Chair of the UN Internet Governance Forum (2005-2010). From 2009 to 2011 he chaired the "Cross Border Internet Expert Group" of the Council of Europe, which drafted the COE Declaration of Internet Governance Principles.

His research work includes more than 100 international publications, including seven books. He also served as a member of several advisory boards of scientific journals. His recent publications include “Sharing Decision Making in Internet Governance”, in William Drake, The Working Group on Internet Governance: 10th Anniversary Reflections (2015), “Internet Fragmentation: An Overview”, World Economic Forum Davos (2016) with Vint Cerf and William Drake) and “Internet Governance Outlook 2017: Nationalistic Hierarchies vs. Multistakeholder Networks”, CircleID (2017).

TOWARDS A HOLISTIC APPROACH FOR INTERNET RELATED PUBLIC POLICY MAKING

CAN THE HELSINKI PROCESS OF THE 1970S BE A SOURCE OF INSPIRATION TO ENHANCE STABILITY IN CYBERSPACE?

Wolfgang Kleinwächter,
Professor Emeritus from the University of Aarhus,
Former Director on the ICANN Board

GCSC **THOUGHT PIECE**
JANUARY 2018

20 years ago, Internet governance[1] was a technical issue with some political implications. Today, Internet governance is a key political issue with some technical components. This shift is challenging the **institutional balance within the global Internet governance ecosystem** and its governmental and non-governmental negotiation mechanisms. Intergovernmental networks like the G20, G7 and BRICS, or organizations like NATO, WTO, ILO and OSCE, which in the past had nothing or only little to do with Internet governance, are now becoming key players. This does not mean that technical organizations like ICANN, IETF, ISOC, RIRs, W3C, IEEE, 3GPP, etc., which dominated the Internet governance discussions in the last two decades, will lose their roles. What we see is a new "Internet governance complexity". The rebalancing of power within the Internet governance ecosystem pushes for innovative approaches to global Internet related public policy making and for enhanced cooperation among governmental and non-governmental stakeholders, as well as for a closer collaboration among both national and global code-makers and law-makers.

Policy making in cyberspace is done by both **state and non-state actors**. The Internet governance working definition, which was adopted by the UN World Summit on the Information Society (WSIS) in Tunis 2005, has singled out "governments, private sector and civil society" as the main stakeholders. Today, the technical-academic community is seen as a fourth key stakeholder. All stakeholders operate in their "respective roles", which means they cannot substitute for each other but have to work hand in hand. They have "to share principles, rules, norms, decision-making procedures and programs". No stakeholder can manage cyberspace alone. All stakeholders are needed to keep the cyberspace open, free, unfragmented and stable.

The "Internet governance ecosystem" is a **layered mechanism**. The WSIS definition differentiates between the "development" and the "use" of the Internet.

1. The "development" of the Internet refers to the lower or technical layer (governance *of* the Internet), the "use" of the Internet refers to the upper or political layer (governance *on* the Internet). This upper layer can be subdivided into three interconnected sub-layers: security, economy, and human rights.
2. Although it is impossible to separate the technical from the political layer, there is also a common understanding, that all layers/sub-layers have to be treated differently, according to the specific nature of the issue at hand. There is no "one size fits all". It is widely accepted that non-state actors are playing a leading role on the technical layer while governments play a leading role on the political layer. However, such a differentiation does not exclude neither governmental involvement on the technical layer nor the involvement of non-state actors on the political layer.

[1] The term "Internet governance" was coined by the Harvard Information Infrastructure Project (HIIP) in the middle of the 1990s. It was used to clarify that the Internet is not managed by governments. The UN World Summit in the Information Society (WSIS) recognized the role of non-governmental stakeholders and adopted in Tunis (2005) a working definition: *"Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet*." The Tunis Agenda also reaffirmed "*that policy authority for Internet-related public policy issues is the sovereign right of States*." When the Internet became more relevant for international security and the global economy, new language was introduced such as "cyber" (used mainly by ministries of foreign affairs, defense and interior) or "digital" (used mainly by ministries of economic affairs, technology and development). Some countries use "ICT technologies" instead of "Internet". The business sector uses "eCommerce". There is no definition of the "Internet of Things" (IOT). The IGF IOT Dynamic Coalition sees IOT as an "application on top of the Domain Name System (DNS)".

There is no agreed definition on "multistakeholderism". The WSIS definition (2005) has introduced the concept of the "respective roles" and the philosophy of "sharing". The NetMundial Declaration (2014) has defined key elements as bottom up, openness, transparency, inclusiveness and human rights-based. In other words, we have some general guidelines for a *multistakeholder approach*, but we do not have a pre-defined single *multistakeholder model*. So far, two different multistakeholder models have emerged: the ***consultative model*** and the ***collaborative model***.

1. In the ***consultative model***, governments "consult" with non-governmental stakeholders, but the final decision-making remains in their hands. The WSIS+10 process from 2015 is a good illustration that such an approach can produce meaningful results. Another good example is the OECD where the Ministerial Meeting takes input from four Advisory Committees. However, the reality is quite often that governments merely pay "lip service" to multistakeholderism when they invite non-state players to consultations, but ignore their advice in decision-making. Thus far, there is no established mechanism – neither in the G7 nor in the G20 where so-called "multistakeholder conferences" were organized in parallel to ministerial meetings for the digital economy – on how non-governmental advice is handled in intergovernmental processes.
2. The ***collaborative model*** goes one step further. In this model, state and non-state actors are operating on an equal footing. Policy development is done through bottom up, open and transparent processes. Decisions are made by rough consensus. The model is based on mutual trust, the "do no harm" principle, the philosophy of "sharing" and the understanding that in an interdependent and interconnected world, every player knows what they have to do. The Internet Governance Forum (IGF), the NetMundial Declaration of Internet Governance principles (2014) and ICANN´s IANA transition (2016) are three successful examples. This model is complex and not easy to explain to outsiders, but the outcome is more sustainable as decisions that are made by one stakeholder group alone.

In the 1990s, there was a clear distinction between the technical layer and the political layer. With less than 100 million Internet users worldwide (out of the total world population of six billion) Internet problems were seen as "sectoral problems" and did not really play a role in the discussion of global political issues as international security, economic development, trade, environment, human rights etc. This has changed. Today we have around 4 billion Internet users and nearly all "traditional" public policy issues have an Internet related component. Internet experts are now included into public policy-making and governments pay closer attention to the discussion about technical issues. This has led to parallel and partly competitive negotiation structures and a clash of cultures.

1. Parallel institutional structures:
   a. The established intergovernmental system of the United Nations emerging after WWII is based on intergovernmental treaties that give organizations a special limited mandate for a clearly defined area. The issues are negotiated by governments alone and the outcomes are legally binding treaties. There is very little to no inter-institutional coordination or cooperation across the various sectors.
   b. Over the last three decades, a complementary system of non-governmental constituencies have emerged where non-state actors from the private sector, civil society and the technical community have built institutions that develop specific policies. The outcomes are

technical code, industry self-regulation or legally non-binding commitments. These platforms are highly interconnected.

   c. As a result, issues such as cybersecurity, eCommerce, privacy, Internet protocols or the DNS are negotiated by different state and non-state groups, which can lead to confusing and contradicting regulations.

2. Clash of cultures:
   a. Negotiations among constituencies are iterative processes that include public consultation. They are open, transparent, bottom up, inclusive, and based on the philosophy of "rough consensus and running code".
   b. Negotiations among governments are very mainly behind closed doors, they are not inclusive, not transparent and are based on majority voting or full consensus.

Global intergovernmental negotiations on disarmament, environment, trade or development are not interconnected. They are managed by different ministries within national governments. There is little to no coordination among the various negotiators. On the Internet, everything is connected with everything. This, a new technical protocol can have major implications for cybersecurity, affects business models, and strengthens or weakens human rights. The same goes for political decisions. The new European General Data Protection Regulation (GDPR), which intends to strengthen the individual right to privacy, affects the business of many Internet companies, digital trade, as well as policing cyberspace and the work of law enforcement agencies.

There is nearly no public policy issue anymore that is not Internet-related. In 2015 the Correspondence Group of the UNCSTD Working Group of Enhanced Cooperation (WGEC) tried to identify Internet-related public policy issues and ended up with a list of more than 600 issues. All those issues can be packed into four baskets:

1. Cybersecurity;
2. Digital Economy;
3. Human Rights;
4. Technology.

For the majority of those issues there are existing platforms where either governments or non-state actors are negotiating norms and regulations. This has led to a very diversified and disconnected tableau of Internet related negotiations and discussions where different constituencies and stakeholders are constrained to their silos – often ignoring what is happening in other silos.[2] There are only a limited number of platforms, such as the IGF, that enable and stimulate cross-sectoral and cross-constituency multistakeholder discussions and a more holistic approach.

Cybersecurity is discussed by the United Nations mainly in the First Committee of the UN General Assembly, the UNGGE, the GGECCW, the UN Security Council Counter Terrorism Committee, the ITU, the Council of Europe, European Union, African Union, Interpol/Europol, the Wassenaar Arrangement, the Global Commission on the Stability of Cyberspace (GCSC), the Global Conference on CyberSpace (GCCS),

[2] Russia proposes a cybersecurity treaty in the UN. Such a treaty would affect global eCommerce and the individual right to freedom of expression; 70 WTO Member States are proposing a digital trade pact. Such a pact would have consequences for cybersecurity and will touch the right to privacy; The UN Special Rapporteur on privacy is proposing a UN convention on surveillance. Such a convention would have implications for cybersecurity and the business model of many global Internet corporations.

the Munich Security Conference (MSC), the Global Forum on Cyber Expertise (GFCE), NATO, WSIS, IGF, OSCE, G7, BRICS, and others. For a number of specific issues there are special negotiation and discussion platforms, such as:

1. Norms of behavior of state and non-state actors in cyberspace: UNGGE, OSCE, G7, BRICS, GCSC, GCCS, WEF;
2. Confidence building measures in cyberspace (CBMs): UNGGE, OSCE, ASEAN, G7, BRICS, GCSC, GCCS;
3. Protection of the public core of the Internet and critical infrastructure as electricity, financial transactions, transportation services and electoral systems: UN, G7, ICANN/PIT, GCSC, GCCS, MSC, NATO;
4. Moratorium for the development of lethal autonomous weapon systems (LAWS) and other Internet based offensive cyber weapons: GGECCW, GCCS;
5. Dual-use technologies: Wassenaar Arrangement, GCSC, GCCS;
6. Fight against cybercrime: Council of Europe, Interpol/Europol, GFCE, GCSC, GCCS, WEF, EU, AU;
7. Fight against the terrorist use of ICTs: UN Security Council Counter Terrorism Committee, Interpol/Europol, GCCS, GCSC, WEF.

Digital economy is discussed by the G20, the G7, WTO, UNCTAD, UNDP, WIPO, UNCITRAL, OECD, the World Economic Forum (WEF), UNCSTD, WSIS, IGF, the International Trademark Association (INTA), ICANN, Trademark Clearinghouse, etc.. For a number of specific issues, there are special negotiation platforms, such as:

1. Digital Trade: G7, G20, WTO, UNCTAD, OECD, WEF, IGF;
2. eCommerce: WTO, UNCTAD, UNDP, UNCITRAL, OECD, WEF;
3. Infrastructure development: UN Regional Commissions, ITU, UNCTAD, IGF, WSIS;
4. Industry 4.0: G20, G7, WEF, IGF, OECD;
5. Internet of Things : G20, G7, ITU-T, IGF, WEF, OECD;
6. Artificial Intelligence :G7, IGF, WEF, OECD;
7. Protection of Intellectual Property: WIPO, WSIS, IGF, INTA, OECD, ICANN/Trademark Clearinghouse.

Human Rights are discussed within the Third Committee of the UN General Assembly, the UN Human Rights Council (HRC Special Rapporteurs for Freedom of Expression and Privacy in the Digital Age), UNESCO, ILO, Council of Europe, OSCE, WSIS, IGF, UNDP, UNCSTD, Freedom Online Coalition (FOC), Reporter without Borders (RWB), APC, Human Rights Watch (HRW), the Global Commission on the Future of Work and others. For a number of specific issues, there are special negotiation and discussion platforms, such as:

1. Access to the Internet: UNESCO, ITU, WSIS, IGF, APC;
2. Freedom of expression: HRC, UNESCO, Council of Europe, OSCE, WSIS, IGF, FOC, RWB, HRW;
3. Privacy in the digital age: HRC, UNESCO, Council of Europe, WSIS, IGF, FOC, ICANN/Whois;
4. Right to education: HRC, UNESCO;
5. Right to culture: HRC, UNESCO;
6. Online Media: HRC, UNESCO, Council of Europe, OSCE;

7. Future of work: HRC, ILO, Global Commission on the Future of Work.

Technical issues are discussed by the so-called I*Organizations such as ICANN, IETF, IAB, ISOC, W3C, RIRs and the IGF but also by intergovernmental organizations including WSIS, ITU and ETSI. For a number of specific issues there are special negotiations and discussion platforms, such as:

1. IP addresses: RIRs, IGF, WSIS, ITU;
2. Domain Name System: ICANN, IGF, WSIS, ITU;
3. Root server system: ICANN/PIT, IGF;
4. Internet protocols: IETF, W3C, IEEE, 3GPP, ITU, ETSI, IGF;
5. IOT: ITU-T, IGF, WSIS;
6. OTT: ITU-T, IGF.

On the one hand, there is an objective need for a holistic approach that links the various intergovernmental and non-governmental negotiations and discussion platforms. On the other hand, it would be an illusion to expect that all those Internet-related public policy and technical issues can be packed into one single negotiation process as it was done under the negotiations for the UN Convention of the Law of the Sea (UNCLOS) or under the United Nations Framework Convention on Climate Change (UNFCCC). A more realistic approach could be the creation of a broad, decentralized and flexible framework to promote and enhance the level of communication and coordination, as well as informal or formal collaboration among the various platforms. Those platforms and negotiation groups could be linked together via "liaisons" and a mechanism of "reciprocal reporting".

Such a framework could emerge both within existing mechanisms such as the IGF, WSIS or NetMundial, but also on top of those mechanisms as a new and independent initiative.[3] To make such a framework workable, it has to give incentives to all stakeholders and to all regions both from the developed as well as the developing world. It has to be based on existing mechanisms and agreements, such as the WSIS documents or the decisions by the UN General Assembly that international law and human rights are relevant both in the offline and the online world.

[3] One source of inspiration could be the „Conference on Security and Cooperation in Europe" (CSCE), the so-called „Helsinki process", of the 1970s. The 1960s saw a growing number of conflicts in the East-West Cold War. To reduce the tensions to avoid a nuclear war, a number of bi- and multilateral treaties and negotiations were initiated, inter alia the Test-Ban Treaty (1963), the Outer Space Treaty (1965), the Non-Proliferation Treaty (1968), the SALT negotiations (1969), the Berlin Agreement (1971) and bilateral treaties between West Germany and the Soviet Union, Poland, the Czechoslovakia and East Germany (1972/1973). All this was channeled into the Conference for Security and Cooperation (CSCE) aimed at the further reduction of tensions within Europe, to enhance cooperation among East and West and to protect human rights. The East had security as its first priority. The West did have human rights as its first priority. But all sides had common interests in a general stabilization of the political landscape and in an enhancement of economic cooperation. The numerous East-West issues were packed into three baskets (Security, Economy, Human Rights), were negotiated individually, but were interconnected, which allowed asymmetric compromises in the negotiation processes (as the British Foreign Minister argued in 1972 that "without eggs in basket 3, there will be no eggs in basket 1"). The CSCE Final Act from 1975 was not a legally binding treaty. However, its political commitments created a rather stable framework which avoided a further growth of East-West tensions with incalculable side effects and the risk of a nuclear war. It paved the way for the democratization processes in the second half of the 1980s and enabled the establishment of the "Organization for Security and Cooperation in Europe" (OSCE), which contributed effectively to peace and international understanding until today. Regardless of some similarities between the CSCE process and a possible CSCC, there are also rather big differences: CSCE/OSCE covers only Europe (from Vladiwostok to Vancouver). A CSCC would have to cover the whole world and give special incentives to developing countries from the Global South and big powers, such as China, Brazil and India, which have been not part of the CSCE. The CSCE/OSCE model is an intergovernmental mechanism. A CSCC would have to be a multistakeholder process. The CSCE was a centralized negotiation platform. A CSCC would have to be designed as a decentralized mechanism.

Such an approach could be framed as a decentralized, informal and global **Conference on Security and Cooperation in Cyberspace (CSCC)**, which could be aimed at the drafting of a "Final Act on Security and Cooperation in Cyberspace" (FASCC) with legally non-binding commitments from governments, the private sector, civil society and the technical community. To design a process for a decentralized, informal and global Conference on Security and Cooperation in Cyberspace (CSCC) and to move towards on outcome document in form of something like a **"Final Act on Security and Cooperation in Cyberspace" (FASCC)** there are four options:

Option 1: Internet Governance Forum (IGF)

The IGF was established by the WSIS in 2005 as a discussion platform – it is not a negotiating body. However, the renewal of the IGF mandate by the 2015 WSIS+10 meeting was linked to the expectation to have more tangible output. The design of the IGF gives the Multistakeholder Advisory Group (MAG), the oversight body for the IGF, a lot of flexibility to orchestrate the discussion in a way that it links existing and isolated intergovernmental and non-governmental negotiation platforms to the multistakeholder environment, which is provided by the IGF and to function like a clearinghouse. The MAG/IGF could invite the various organizations, which negotiate issues from the four baskets, to report on an annual basis to the IGF, to discuss the reports in a multistakeholder environment and to send "messages" back to the negotiation platforms.

Option 2: The WSIS +20 process

The next WSIS review is scheduled for 2025 (WSIS+20). One could imagine to restructure the preparatory process going beyond the Tunis Agenda and using the "four baskets approach". This would enable governmental and non-governmental stakeholders to negotiate new political commitments within a new WSIS+20 Declaration. Such commitments would not substitute intergovernmental treaties which are negotiated in special committees among governments for cybersecurity, digital trade or human rights, but they would connect the various issues into a comprehensive Internet Governance Policy Framework – something like a CSCC – and would broaden the horizon for treaty makers by creating more awareness about possible unintended side effects of sectoral intergovernmental regulations.

Option 3: The Net Mundial +5 process

The Global Multistakeholder NetMundial Conference (Sao Paulo 2014) adopted a "Internet Governance Roadmap". This Roadmap could be used as a starting point for the launch of a CSCC. There are discussions to convene a NetMundial+5 conference in 2019 (as a pre-event to the 14th IGF scheduled in Berlin in November 2019) that will review the implementation of the NetMundial Declaration of Internet Governance Principles as well as the Roadmap.

Option 4: A new independent process

One could also imagine that state and non-state actors agree to establish a new independent process towards a CSCC, aimed at the elaboration of a comprehensive "Final Act on Security and Cooperation in Cyberspace".

SECRETARIAT

The Hague Centre for Strategic Studies

EastWest INSTITUTE

PARTNERS

Ministry of Foreign Affairs

CSA SINGAPORE

Microsoft

Internet Society

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

SPONSORS

Ministry of Foreign Affairs
Of Estonia

SUPPORTERS

Black Hat USA
Packet Clearing House