GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

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

Submission from the Global Commission on the Stability of Cyberspace (GCSC) to the Internet Governance Forum Best Practice Forum on Cybersecurity Culture, Norms and Values (2018)

1. Foreword

The Global Commission on the Stability of Cyberspace (GCSC) appreciates the opportunity to contribute to the work of the Internet Governance Forum (IGF) Best Practice Forum Working Group on "Cybersecurity Culture, Norms and Values." The Commission underlines the important work and role of the IGF's Best Practice Forum in engaging a wide range of stakeholders on matters pertaining to cybersecurity norms. The mission and mandate of the Commission are strongly aligned with the objective of the IGF in promoting multi-stakeholder engagement on issues essential to maintaining an open, free and secure Internet.

From its inception, the Global Commission on the Stability of Cyberspace aims to bring the expertise, knowledge and perspectives from non-state stakeholders into the traditionally state-driven dialogues of international peace and security in cyberspace. Ensuring a diversity of perspectives in this dialogue, representing different stakeholders in government, civil society and the private sector, is essential for the online environment to continue to thrive.

Upon request, this submission will outline the context, mission and methodology of the GCSC in developing norms of responsible behavior and how they fit into the wider security architecture in cyberspace, which we hope can serve as input into the final output of the IGF Best Practice Forum.

2. The GCSC – Working Across the Cyber Regime Complex

From its very beginnings cyberspace has been loosely governed. This was by design, helped encourage the fledging technology and was likely critical for its rapid growth. Cyberspace has created unprecedented social and economic and social benefits, but it also creates real risks and challenges for international peace and stability. While cyberspace is no longer the "Wild West," powerful nations still see it as an unconstrained arena for conflict. Dangerous actions by both state and non-state actors produce a growing sense of concern in the international community and the public at large.

These concerns have created widespread demand for better and more explicit governance structures for what has become an essential global infrastructure. However, the range of actors, their relevant responsibilities and their activities make for a highly complex ecosystem. A number of initiatives – many of them claiming a security mandate of some sort – take place in specific

"regimes," such as within law enforcement, or incident response. Each effectively engages in governance within a specific thematic area, defining accepted standards, policies, laws or similar.

This process of formation and governance is encapsulated in a number of different assumed responsibilities and activities – ranging from non-state-led processes (e.g. technical Internet governance) to state-led processes on international security issues (e.g. the UN Group of Governmental Experts). Together this "galaxy" of initiatives forms the "cyber regime complex", as elucidated by Joseph S. Nye in a publication of the Global Commission on Internet Governance[1], and in subsequent publications since then.[2] One of its most important features is that it is very much multi-stakeholder in its composition – the government, the private sector and the civil society (which includes the technical community as well as academia and NGOs) all play a role – very often together.

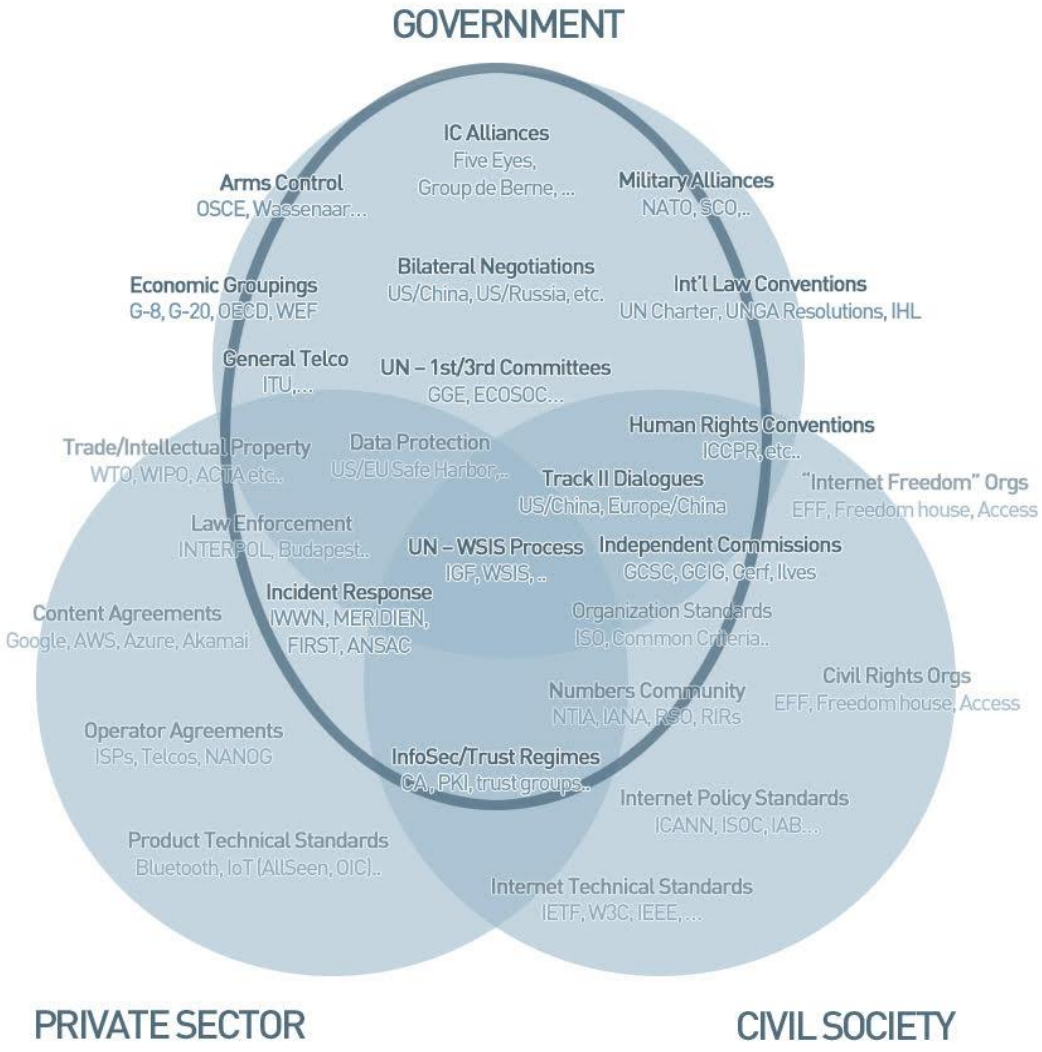

Figure 1 The Cyber Regime Complex by stakeholder group: the "international cybersecurity" cluster.[3]

[1] Joseph S. Nye, Jr. (2014), "The Regime Complex for Managing Global Cyber Activities," Global Commission on Internet Governance.
[2] Alexander Klimburg and Louk Faesen (2018), "A Balance of Power in Cyberspace" European Cybersecurity Journal Volume 3 (2018) Issue 4.
[3] Ibid.

Given the analysis that many of the regimes are unique and autonomous, but also often work at odds, it is becoming evident that finding a mode of coherence amongst them is a critical step in being able to define actionable international cybersecurity measures, irrespective of whether they are mainly technical, legal, or political.

Unlocking the synergetic (cooperative) potential of this regime complex is key to achieving what the U.S. State Department International Security Advisory Board originally referred to as "international cyber stability":

> "A stable international cyberspace can be defined as an environment where all participants can positively and dependably enjoy its benefits, where there are incentives for cooperation and avoidance of conflict, and where disincentives for engaging in malicious cyber activity apply. A stable cyber framework has geopolitical, economic, technological, and legal elements."[4]

The various 'elements' referred to here have further been defined by the international relations scholar Joseph S. Nye as forming a 'regime complex' of various interlocking but separate governance processes that together define cyberspace.[5] This regime complex is only partially influenced by state actors, for instance within 'international cybersecurity regimes' (e.g. within the UN and diplomatic processes on regional and bilateral levels). As is remarked within the U.S. State Department report, the role of governments within other processes or regimes is much more limited – the private sector and civil society both generate products, common practices, and norms of behavior largely separate from government involvement, although these developments can have significant impacts on national security. Therefore, despite its traditional dominance of all questions related to international peace and security, the role of government within the overall cyberspace regime complex is no greater to that of the private sector or civil society. The state-oriented regimes do not necessarily have the ability to 'speak' on the behalf of other, equally crucial, regimes. This creates a situation nearly unique in international peace and security*: government cannot decide all aspects of the international cybersecurity domain itself, as responsibility and ownership for this domain is shared with non-state actors*.

Establishing finely-delineated legal responsibilities for the various regimes in cyberspace is often not possible. Indeed, legal agreements have proven to be difficult even between governments. As a consequence, arrangements outside or next to the law have become a common practice. "Norms of behavior" have become a common standard for agreeing on what constitutes acceptable action in cyberspace. Due to the shared responsibility in cyberspace between the various regimes, both state and non-state norms can and do overlap.

One of the challenges of agreeing on norms of behavior in cyberspace is that norms - and the associated practical implementation measures, such as Confidence-Building Measures (CBMs) – are sometimes formulated by one set of actors but expected to be executed by another. This requires that the actor groups, regimes, and initiatives fully recognize each other's mandate or legitimacy. This is not automatically the case. Government actors can struggle to accept the legitimacy of individual engineers who build the Internet largely in their spare time, while the

[4] U.S. State Department International Security Advisory Board (2014) "Report on a Framework for International Cyber Stability", available at http://www.state.gov/documents/organization/229235.pdf.
[5] Joseph S. Nye, Jr. (2014), "The Regime Complex for Managing Global Cyber Activities," Global Commission on Internet Governance.

same non-state actors are often scornful of the knowledge, intention, or capabilities of government.

Working across the regime complex is therefore primarily a question of accepting mutual legitimacy. Any norm, project or initiative that seeks to have a truly global reach and effect on cyberspace must have the support of key actors across the regime complex to succeed. These actors are considered to be legitimate either because of their ability to be representative of their constituents (be it members, citizens, or customers), knowledgeable on the technical details within their field, or the ability to practically effect change. Accepting any one of these definitions of legitimacy is the equivalent to trusting the verdict of these actors to at least be relevant within the wider discourse, and, as the U.S. State department pointed out within their 2014 report, trust among these different state and non-state actors is key to cyber stability.

If they are brought together in an appropriate forum, such a collection of actors could effectively provide much-needed judgement on numerous norms, projects, and policy and diplomatic initiatives that previously would have not been widely consulted. Such a forum could provide a definitive, authoritative assessment of what works, and what would not work, in cyberspace – separate from any vested interests or indeed political posturing. This forum of "wise men and women" of cyberspace could provide an independent and final voice on any specific idea, norms or policy initiative on cyberspace, and thus endow it with much-needed legitimacy.

The Global Commission on the Stability of Cyberspace is this forum. The 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.

3. The GCSC Method – Bottom-Up to Top-Down

Norms are foundational for better governance, and therefore the initial focus of our work. In international security, norms can be fairly abstract – for instance, the 2015 UN GGE report stated that states should not "interfere with critical infrastructure", nor should they "conduct or knowingly support activity to harm the information systems of the authorized emergency response teams of another State. A State should neither use authorized emergency response teams to engage in malicious international activity."[6] In industry and civil society for instance, norms may be much more practical (where they are usually called CBMs in international security), for instance the MANRS (Mutually Agreed Norms for Routing Security). Indeed some might say that technical fixes such as Source Address Validation (SAV) is a norm, as is BPC-38. Others might say that these are all the same thing – norms – and that it's crucial they are actionable and intelligible, or that they have been agreed as necessary. Norms therefore are actually at the beginning – they form a test of "what needs to be done" – a practical sense test of what practical and operational steps need to be undertaken to achieve some measure of "cyber stability" that should help us understand, what cyber stability actually is.

Accordingly, the Global Commission on the Stability of Cyberspace (GCSC) has approached its deliberation in a bottom-up to top-down manner. Firstly, the Commission is to identify operational norms that meet the most obvious urgent international cybersecurity needs as

[6] The Report of the Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security, United Nations General Assembly, July 22, 2015 (A/70/174), available at .http://undocs.org/A/70/174.

expressed by its members. Secondly, it will extrapolate from these norms to establish its own working definition of cyber stability, as well as the associated principles. Furthermore, it will use these principles to develop a clearer understanding of what the wider international peace and security architecture needs to do to meet that definition. Finally, it will offer recommendations to state and non-state stakeholders on how this can be accomplished. Taken together, the Commission aims to have a significant impact on the international peace and security governance architecture as it is relevant to cyberspace.

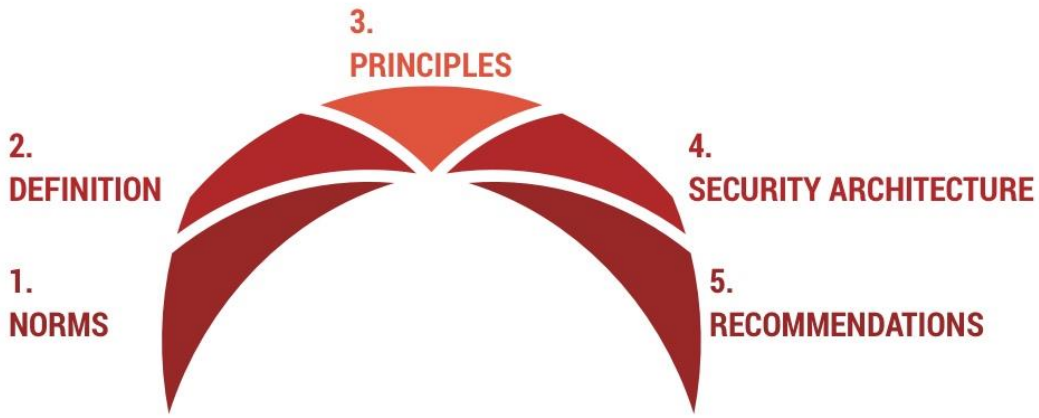

Figure 2 GCSC Methodology bottom-up to top-down

Throughout our deliberations, the GCSC is guided by significant shared core beliefs. These include the importance of a democratic, multi-stakeholder approach to governance, the necessity to promote development and growth, the need to balance rights and responsibilities for both state and non-state actors, and the centrality of cyberspace remaining open and unimpeded in its operations. We therefore also aim to expand the global understanding of responsible behavior in cyberspace for both states and non-state actors.

We did not begin our work in a vacuum. As the background paper of the IGF BPF on Cybersecurity has outlined, various stakeholders have identified possible norms and principles. These include the United Nations Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security (UN GGE), the G20, the G7, and regional organizations, as well as non-state norms developed by Microsoft, and ISOC, to name but a few. It has also greatly benefited from the work done within the Internet governance ecosystem, including the work of the NetMundial Initiative well as the many initiatives occurring within the wider Internet Governance Forum (IGF) ecosystem.

4. Norms

The mandate of the Global Commission on the Stability of Cyberspace is to develop proposals for norms and policies to enhance international security and stability in cyberspace.

The GCSC's first task is therefore to examine how existing norms can be applied to cyberspace; where new norms are needed, and how to put these norms into operation and use. A norm works best when the international community is seized by it, when it shapes both the behavior of public and private institutions and the decisions of national leaders, and when it makes clear to all that some actions fall outside the bounds of what is acceptable.

As a first step, recognizing the global reliance on cyberspace, the increasing dependence of other infrastructures on its reliability, and the potentially dramatic consequences of its disruption, the Commission urges for the protection of the Public Core of the Internet as the first operational norm that meets the most obvious urgent international norm that is critical of cyberspace. Secondly, the GCSC identified the protection of the electoral infrastructure, which advocates a prohibition on the disruption of elections through cyber attacks on its technical infrastructure, as an urgent norm that is critical in cyberspace. Moving forward, the Commission is set to publish a number of additional norms of responsible behavior. Once finalized, the norms will urge governments and others to avoid taking actions that would substantially impair the stability of cyberspace, including inserting vulnerabilities into products and services, commandeering others' devices to create botnets, and allowing non-state actors to conduct offensive cyber operations. The norms will also urge action to preserve the stability of cyberspace, including establishing vulnerabilities equities processes and enacting basic cyber hygiene.

Figure 3 Spectrum of GCSC norms ranging from norms that are "critical of cyberspace" to "critical in cyberspace"

Prior to the publication of the Call to Protect the Public Core of the Internet, the Commission was informed by state and non-state experts through the public CyberStability Hearings, as well as the briefings and memos developed by independent researchers working within the GCSC Research Advisory Group. The research was commissioned by the GCSC in a Request for Proposal after its Commission Meeting in Tallinn in June 2017. The Commissioners selected the winning proposals at the Commission Meeting in Las Vegas in July 2017. The researchers received the funding associated with the Request for Proposal and were invited to present their work to the Commissioners during the Commission Meeting in New Delhi in November 2017.

Since the publication of the public core norm at the GCCS in September 2017 in New Delhi, the Commission as a whole advocated for the norm at government, corporate and civil society headquarters and forums. As input to its process, a working group of the GCSC conducted a broad survey of experts on communications infrastructure and cyber defense to assess which infrastructures were deemed most worthy of protection. Accordingly, the Commission defines the phrase "the public core of the Internet" to include packet routing and forwarding, naming and numbering systems, the cryptographic mechanisms of security and identity, and physical transmission media. One of the most concrete outcomes since its publication is the European Parliament's support for the GCSC and the public core norm in its amendments to the resolution and report on cyber defence (2018/2004(INI)).

5. A Definition and Principles for Stability in Cyberspace, its Place in the Wider Security Architecture, and Recommendations Moving Forward

The GCSC's work has focused on developing recommendations for norms of responsible behavior in cyberspace, to provide stability and influence the conduct of both states and ICT companies in ways that complement and reinforce norms developed in the United Nations and elsewhere. Our future work will identify governance frameworks in which to embed norms and anchor stability in cyberspace.

There are precedents for the GCSC's work. The Brundtland Commission created norms for Sustainable Development. A Carnegie Commission on Preventing Deadly Conflict led to the International Commission on Intervention and State Sovereignty and a commitment by all UN member states on the duty to prevent and protect against war crimes, genocide, ethnic cleansing and other crimes against humanity. The Ilves Commission helped set the framework for the NetMundial Initiative. The Brandt and Palme Commissions represented important steps both in development and disarmament, respectively. These nongovernmental groups reshaped global discussion of responsible behavior and created new norms for unprecedented international problems.

We hope to do the same. Our proposed norms address immediate issues created in recent years by the use of cyberspace. We support the work of the GGE and affirm the findings of the GGE Reports, in particular its framework on the applicability of existing international norms, law and practices. We seek to amplify and expand this initial normative structure in ways intended to complement and reinforce existing areas of agreement and point the way to new opportunities for increasing the stability of cyberspace.