Policy Brief | 17

Cyber Governance:

Challenges, Solutions, and Lessons for Effective Global Governance

November 2015

Sash Jayawardane
Researcher, Global Governance program

Joris Larik
Senior Researcher, Global Governance Program;
Assistant Professor, Leiden University

Erin Jackson
Project Associate, Commission on
Global Security Justice & Governance

The Hague Institute
for Global Justice

Cyber Governance:

Challenges, Solutions, and Lessons for Effective Global Governance

Executive Summary

Cyberspace permeates global social and economic relations in the 21st Century. It is an integral part of the critical infrastructure on which modern societies depend and has revolutionized how we communicate and socialize. The governance of cyberspace is, therefore, an indispensable component of global governance, and a testing ground for new models of cooperation that could be adapted for effective governance in other areas.

The purpose of this policy brief is to provide policymakers with insights on how to improve the effectiveness of cyber governance institutions and processes. These insights could also inform efforts to improve global governance institutions and processes more broadly. The brief considers two principal questions: *Who* should govern cyberspace, and *how*? In response to the former question, the authors review multistakeholder models of governance and provide recommendations for their improvement. These include: greater transparency of decision-making processes, with a prohibition on vetoes; dedicating financial resources to the empowerment of disadvantaged stakeholders; and allocating leadership positions in an equitable manner. In response to the latter question, the authors assess formal and informal approaches to governance in cyberspace, concluding that cyberspace should be governed through a combination of both. That is, a flexible, incremental and sectoral approach to strengthening the rule of law in cyberspace through international treaty-making should be complemented by efforts to build trust and consensus through the development, diffusion and institutionalization of norms for responsible behavior in cyberspace, as well as related confidence- and capacity-building measures. Taken together, these recommendations aim to foster common understanding and enhance security and the rule of law in cyberspace.

This policy brief draws on The Hague Institute's work on the *Global Governance Reform Initiative* (GGRI) project and the *Global Conference on Cyberspace* (GCCS), hosted by the Kingdom of the Netherlands in April 2015. The GGRI project is a collaborative effort between The Hague Institute, The Ministry of Foreign Affairs of the Netherlands, and the Observer Research Foundation (New Delhi).

Introduction

The governance of cyberspace is complex and contested. The decentralized nature of the medium – which is largely owned and operated by the private sector, but is increasingly of consequence and interest to governments and civil society – poses a challenge to traditional methods of global governance, which are inclined to be state-centric and somewhat inflexible. This policy brief aims to provide policymakers with insights on how to improve the effectiveness of cyber governance institutions and processes. It focuses particularly on insights that may be applicable to global governance institutions and processes more generally.

The first part of this brief asks *who* should be involved in cyber governance, and examines multistakeholder models of governance. It provides an overview of several multistakeholder models that are currently in use, assessing their strengths and weaknesses. The section concludes with policy recommendations to improve multistakeholder governance, both in cyberspace and more generally. The subsequent sections of the brief focus on *how* cyberspace should be governed. The discussion begins with formal governance arrangements such as international treaties, and proposes that a flexible, incremental and sectoral approach to treaty-making can help overcome the reluctance of stakeholders to make legally-binding international commitments. This would strengthen the rule of law in cyberspace and demonstrate the relevance of existing international law in non-traditional areas of global governance.

The final section focuses on informal approaches to cyber governance, which include norm development and confidence- and capacity-building measures. The discussion here focuses on how such approaches can complement formal governance by building trust and consensus through the development, diffusion and institutionalization of norms for responsible behavior in cyberspace. Relevant policy recommendations are included at the end of each section and are summarized in the conclusion.

1. Who should govern cyberspace? An analysis of multistakeholder governance

Contemporary understandings of what constitutes global governance are increasingly less state-centric, recognizing that other stakeholders can play an important role. Multistakeholder approaches to governance can empower non-state actors to participate in the development and implementation of international public policy, thereby increasing the inclusiveness and representativeness of governance processes.

The governance of cyberspace is a particularly important case study of multistakeholder governance, given its highly decentralized nature. Internet governance scholar Laura DeNardis describes multistakeholderism in cyberspace as "a constantly shifting balance of powers between private industry, international technical governance institutions, governments and civil society"[1] For effective governance,

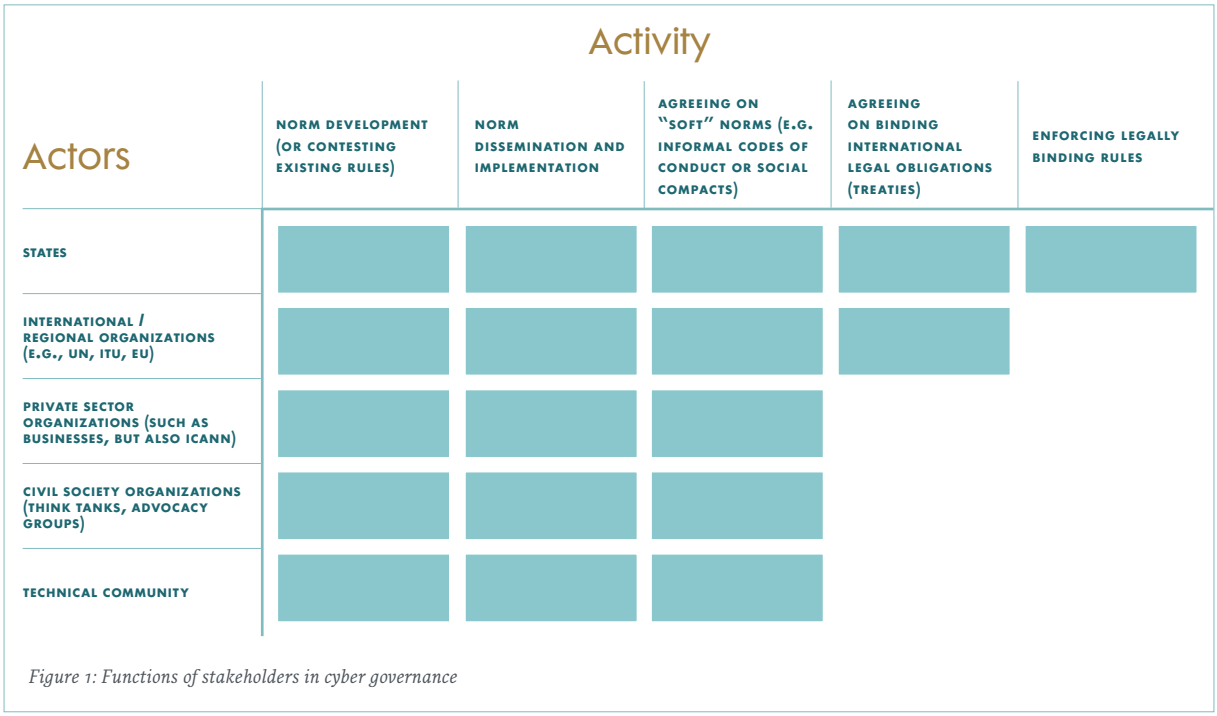

Figure 1: Functions of stakeholders in cyber governance

multistakeholderism should be understood not as a value in itself, but rather "a question of what form of administration is necessary in any particular context."[2] Multistakeholderism therefore does not envision that all stakeholders should participate in the same manner and to the same degree in all governance matters. For example, technical matters related to the smooth operation of cyberspace are largely handled by the private sector, while only states – and to some extent international organizations – can be party to international treaties regulating cyberspace. Non-states actors can sign and support "soft" instruments such as the NETmundial Multistakeholder Statement, and play a critical role in shaping, disseminating and institutionalizing norms of behavior in cyberspace (see also Figure 1 above). Regardless of the particular configuration of stakeholders necessary for a specific governance task, establishing legitimate public policy requires that governance processes and mechanisms be both transparent and accountable.[3]

The evolution of governance arrangements in cyberspace has thus far been directed largely by stakeholders (primarily states and the private sector) in the United States and other Western countries. However, there is growing acceptance that the future of cyber governance will be heavily influenced by stakeholders in non-Western nations, such as Brazil, China and India, which have rapidly growing populations of Internet users and provide a large portion of ICT products and services. Even with multistakeholder models of governance in place, countries and other stakeholders that are relative newcomers to cyber governance are often at a disadvantage. The disparity between the ability of stakeholders from developed and developing countries to participate effectively in cyber governance is particularly evident.[4] Below, we consider several multistakeholder cyber governance platforms and suggest how these could be improved in terms of transparency and accountability, as well as empowering previously disadvantaged stakeholders to play an effective role in cyber governance.

1.1 Multistakeholder models of cyber governance: Strengths and weaknesses

Contemporary cyber governance encompasses several multistakeholder governance fora and processes, including the Internet Corporation for Assigned Names and Numbers (ICANN), the International Telecommunications Union (ITU), the Internet Governance Forum (IGF), and the Global Multistakeholder Meeting on the Future of Internet Governance (NETmundial). Each governance mechanism has unique strengths and weaknesses, while all require improvement to be legitimate and effective.

ICANN is a private, nonprofit organization, which performs key technical tasks to ensure the smooth functioning of the Internet. In March 2014, responding partly to concerns about the predominant position of the US in ICANN, the US National Telecommunications & Information Administration (NTIA) announced its decision to transfer its stewardship of key Internet domain name functions within ICANN to the global multistakeholder community. In theory, ICANN takes a community-based, consensus-driven approach to policymaking through open discussion of its policies. To encourage wide participation, ICANN's annual meeting is mandated to take place in different geographical regions and is free and open to all participants, including the public and private sectors as well as technical experts. During this meeting, any participant can use the Public Forum session to address a point directly to members of the ICANN community and its Board. However, effective participation is often deterred by several factors, including colloquial use of the English language and Internet availability asymmetries.[5]
More importantly, ICANN has been heavily criticized for lacking accountability. It has an undefined membership, which exerts no control over a Board that is appointed "indirectly by a nominating committee composed of ICANN insiders."[6] Weak review and appeal procedures for Board decisions, i.e. non-binding requests to reconsider these decisions, make it difficult to hold the ICANN Board accountable for its decisions and actions.[7]

The **ITU** is the specialized UN body for information and communications technologies (ICTs) that allocates global radio spectrum and satellite orbits and develops technical standards. As a UN body, the ITU is mandated to engage with all nation states. Thus, Least Developed Countries, which primarily engage in cyber governance through the ITU, often see it as "the most appropriate forum for governing global electronic networks, including the Internet."[8] However, the ITU's claim to be a multistakeholder governance forum is somewhat hollow, as only governments formally perform decision-making functions. In recent years, part of the Union's decision-making has been partially delegated to Study Groups whose decisions can be final, but the membership of these groups is drawn largely from telecommunications companies and their suppliers.[9] There is limited participation of civil society organizations, in stark contrast to other cyber governance fora that are open and do not require membership for participation.

The **IGF**, created by the World Summit on the Information Society in 2006, brings together diverse stakeholders to annual meetings about public policy issues pertaining to the Internet under the aegis of the UN. It has been praised as "a laboratory for new modalities to organize the international community."[10] As a non-binding forum for debate on Internet governance policy,[11] best practices and emerging issues, the IGF is more flexible than a UN summit. It is an open forum for "all people with a stake in Internet governance." As such, all participants have the same access and speaking rights, and only online registration is required to participate.
This enables top-down as well as bottom-up

initiatives. There has been strong support for the renewal of the IGF's mandate beyond 2015, which is to be decided on by the UN General Assembly in December 2015.[12] However, some argue that the IGF's forums and symbolic interactions often seem theatrical, and do not focus on producing specific policy outcomes, which pushes the IGF (a forum with no negotiated outcome or decision-making mandate) to the fringes of the core policy debates.[13] Without the authority to establish policies or regulations, it is "unable to influence significantly the hard issues and choices at stake."[14]

NETmundial, which took place in April 2014, is widely considered to have been a successful process of multistakeholder engagement on cyber governance issues. Following revelations of large-scale data surveillance undertaken by the US National Security Agency, the Brazilian government initiated NETmundial, which brought together four groups of stakeholders (governments, the private sector, civil society and the academic/technical community) in quasi-equal numbers, with three levels of participation: content submissions through an online platform; online public comments on a draft of the outcome statement; and open-microphone sessions for participants to directly address the plenary. In addition, the drafting sessions took place in the public eye, making them more transparent.

The NETmundial Multistakeholder Statement drew upon two days of deliberations involving over 900 participants and reinforced the concept of multistakeholderism, stating that "Internet governance should be built on democratic, multistakeholder processes, ensuring the meaningful and accountable participation of all stakeholders ...The respective roles and responsibilities of stakeholders should be interpreted in a flexible manner with reference to the issue under discussion."[15] However, in its assessment of NETmundial, the Association for Progressive Communications noted the influence of powerful governments, who demanded last minute changes (or informal veto) to the pre-final text presented to the High-level Multistakeholder Committee.[16] Despite its successes, NETmundial could not forge complete consensus as India, Cuba and Russia refused to sign the outcome document.

1.2 Improving multistakeholder governance in cyberspace

Multistakeholderism in cyberspace can increase representativeness and effectiveness in the governance of a complex domain by leveling the playing field, preventing the capture of cyberspace by any one type of stakeholder, and allowing different types of stakeholders authority over aspects of governance that they are best equipped to handle. However, multistakeholder governance also presents a number of challenges that must be addressed. Key challenges emerging from multistakeholder governance in cyberspace, which apply to global governance more generally, include the lack of transparency in governance processes; the unequal representation of stakeholders; and the varying degrees of influence that stakeholders wield in shaping international public policy.

The effectiveness and legitimacy of multistakeholder governance processes are often undermined by a lack of transparency and failure to provide stakeholders with proper access to relevant information. Organizational rules of procedure are "usually set by those that hold power and are not subject [to] negotiation between the different stakeholders."[17] For example, although it is an open forum, IGF processes have been criticized for providing asymmetrical access to documents (in favour of governments over other stakeholders) and making decisions behind closed doors.[18] Though many institutions document their policy processes, decisions can still be taken in informal or private settings, giving powerful players such as governments direct channels of influence.[19]

It is important to recognize that various degrees of participation can exist in multistakeholder cyber governance mechanisms. In governance structures such as the ITU, states hold explicit decision-making power and are thus unequal to other stakeholders. Even when all stakeholders theoretically enjoy equal status, however, genuine participation can prove elusive. NETmundial was criticized for not facilitating "full participation" – "a process where each individual member of a decision-making body has equal power to determine the outcome of a decision"[20] – of all stakeholders. Indeed, one representative of civil society opined that the meeting failed to sufficiently move beyond the status quo in terms of balancing the power and influence of different stakeholder groups.[21]

Regarding the degree of influence wielded by different stakeholders in cyber governance, there is dispute about whether multistakeholder arrangements enable all stakeholders to participate in a meaningful way. For example, African countries lack representation in leadership positions within the structure of ICANN, and African civil society groups and representatives of industry also have minimal participation.[22] Additionally, civil society participation in cyber governance mechanisms has been characterized by some as "tokenism," i.e. participation without the possibility of making an actual impact.[23] Civil society participation encounters further difficulties when technical specialists become proxies for civil society due to a lack of readily available expertise.[24]

To address the multitude of factors that impede the genuine and effective participation of all stakeholders in cyber governance mechanisms, and indeed in global governance mechanisms more broadly, efforts must be made to ensure that stakeholders not only have a seat at the table, but are also empowered to shape and implement international public policy. To this end, the following recommendations should be considered:

- **Transparency:** Decision-making processes should be transparent, and decisions subject to review; decision-makers should be held accountable for their decisions by the membership of the relevant governance mechanism; and no stakeholder group should possess formal or informal veto power, which can undermine the inclusive and democratic nature of multistakeholder governance processes.
- **Empowering disadvantaged stakeholders:** Multistakeholder governance mechanisms should allocate dedicated financial resources to develop the capacities of state and non-state actors that are unable to participate in governance processes in a meaningful way due to factors including the lack of financial resources and/or technical knowledge.
- **Equitable participation:** Leadership positions within governance mechanisms should rotate and be allocated in an equitable manner that prevents the formation of cliques, and ensures that the voices of all stakeholders, including civil society and the private sector, are heard.

2. How should cyberspace be governed? Formal approaches: Treaties and the rule of law in cyberspace

Multistakeholder models of governance improve inclusiveness and representativeness in cyber governance. However, such models alone cannot guarantee security and promote the rule of law in cyberspace. While the need to strengthen the rule of law in cyberspace is widely recognized, international legal commitments in this area remain rare. The reluctance of states to make legally-binding commitments is unsurprising – the ubiquitous nature of cyberspace means that how it is governed has important implications for the security, economic prosperity and political stability of states. However, cyberspace does not exist in a legal vacuum, and must contend with the international legal regimes that play a critical role in global governance in the 21st Century. This section proposes a flexible, sectoral approach to achieving legally-binding commitments regarding "rules of the road" in cyberspace to ensure this domain will be "free, open and secure."[25]

2.1 "Pactophobia" and the international rule of law in cyberspace

"Pactomania" is the term used by historians to denote periods of extensive international treaty-making. Cyber governance, however, is characterized by the opposite phenomenon: "pactophobia," or a fear of committing to international treaties. Despite a wealth of (non-binding) statements regarding the governance of cyberspace (e.g. the NETmundial Multistakeholder Statement, the International Code of Conduct on Information Security, the Tallinn Manual (2.0), or Microsoft's International Cyber Security Norms), binding international agreements remain scarce. A notable exception is the Budapest Convention on Cybercrime.[26]

The reluctance vis-à-vis international treaties in cyberspace can be attributed to several factors, including reluctance amongst advanced cyber powers to limit their options for action in cyberspace, and the differing priorities of such states, which are a function of security and economic imperatives. For example, Western nations are particularly concerned with guarding against copyright infringement and industrial espionage, while protecting the freedom of expression online. States such as Russia and China, however, are preoccupied with the notion of "information security," while India is focusing on transforming public services using information technology as part of Prime Minister Modi's "Digital India" program. These diverse, and sometimes competing, national priorities cannot be reconciled effectively by informal means alone.

That existing international law is applicable to cyberspace has been affirmed clearly, in particular by the United Nations Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security.[27] The UN GGE is now engaged in determining exactly how international law can be applied to cyberspace.

The application of existing legal principles to a new domain in this manner is called "grafting." Furthermore, at the national level, numerous countries are now enacting cyber legislation covering issues such as cybercrime and data protection, which may ultimately lead to general principles of international law.

Failing to place cyber governance concretely within the framework of international law undermines the possibility of developing a coherent strategy for governing this critical global resource, as well as for shaping expectations among key players. Moreover, it risks eroding the legitimacy and relevance of international law in framing contemporary challenges.

2.2 Flexible and sectoral approach

Overcoming "pactophobia" and making meaningful progress in promoting the rule of law in cyberspace requires acknowledgement that a "free, open and secure Internet for the benefit of all"[28] is a matter of such global significance that it merits international codification. This means moving beyond simply adding "cyber labels" to existing international rules, and articulating clearly how existing and emerging laws apply to cyberspace. Policymakers need to move from "grafting" to drafting international legal instruments specifically designed for governing cyberspace.

In this brief, we propose two principal means of overcoming "pactophobia" and progressing towards the effective governance of cyberspace: (1) making full use of the flexibility provided under international treaty law; and (2) adopting a sectoral rather than a comprehensive approach to treaty-making.

Those who doubt that international treaties are a viable means of governing cyberspace often fail to appreciate the inherent flexibility of international agreements. The International Law of Treaties, as laid down in the Vienna Convention on the Law of Treaties,[29] offers a number of ways to make treaties more acceptable to potential signatories. These include opt-outs, political offence exceptions, reservations, and termination clauses. The Budapest Convention on Cybercrime makes ample use of such clauses and serves as a useful example here.

- **Opt-out** clauses allow parties to a treaty to abstain from applying certain parts of the treaty. For instance, the Budapest Convention sets out a list of offences related to child pornography that are to be criminalized under domestic law (Article 9, Budapest Convention). Whereas all parties have to criminalize "offering or making available child pornography through a computer system," the Convention leaves to the discretion of the parties whether to apply provisions on criminalizing, for instance, possession of child pornography in a computer system or data storage medium.
- **Political** offence clauses allow a party to refuse to cooperate with another state in matters such as extradition (Article 27). Likely scenarios for the invocation of exceptions would involve treason, espionage and sedition.
- **Reservations** can be issued by states when signing up to a treaty to exclude or modify the legal effect of certain provisions. In order to limit the potential for abuse, the issuing of reservations can be prohibited for certain core provisions of a treaty, which is the case for the Budapest Convention, which uses a positive list of articles which allow reservations, while disallowing them elsewhere (Article 42). For instance, no reservations are allowed with regard to criminalizing "systems interference" (Article 5), for instance by denial of service (DOS) attacks or computer-related fraud (Article 8).
- **Termination** clauses offer states the option of withdrawing from an international agreement. In the Budapest Convention, termination "shall become effective on the first day of the month following the expiration

of a period of three months after the date of receipt of the notification by the Secretary General of the Council of Europe" (Article 47). No country, therefore, is eternally bound by a treaty.

The second means of achieving international legal codification with regard to cyber issues is adopting an incremental, sectoral approach to treaty-making. This approach can be modeled on the international anti-terrorism treaty regime,[30] and can take the Budapest Convention as a starting point. This involves, in the first instance, making use of the flexibility afforded by international treaty law to promote ratification of existing agreements by more countries. In addition, policymakers should carefully select specific cyber issues on which there is some consensus as a basis for drafting viable new agreements.

Cyber issues on which sectoral agreements could focus include: cyber security strategies and best practices; cyber capacity-building initiatives; technical assistance programs for enhancing access in remote and underdeveloped areas; regulation of dual-use cyber technologies; and basic rules of cyber warfare (i.e. turning (parts of) the Tallinn Manual into a treaty). Sectoral agreements can help forge broader consensus and serve as stepping stones towards a global, comprehensive set of rules, such as a cyber equivalent to the United Nations Convention for the Law of the Sea.

There are, of course, limits to what governance through legally-binding agreements can achieve. To be effective, treaties must be enforced and compliance monitored. Moreover, states – which are the traditional parties to international treaties – are not the only players to be reckoned with in cyberspace. International agreements that cannot regulate the behavior of the private sector in cyberspace are likely to fail. Despite these challenges, the above discussion highlights how international law can be harnessed to help govern this vast and complex domain. Three principal policy recommendations emerge:

- **Harness fully the flexibility of international treaty law to create viable coalitions of states to draft, sign and ratify international agreements.**
- **Adopt an incremental, sectoral approach to developing new treaties, selecting specific themes and issues on which a significant degree of consensus already exists.**
- **Accept that a comprehensive treaty for cyber governance is a distant goal, towards which sectoral agreements can serve as stepping stones.**

While flexible international agreements that adopt an incremental, sectoral approach are a promising means of governing cyberspace, they are not the only means of doing so. Ideally, such binding agreements should operate in conjunction with other, informal modes of governance to which the discussion now turns.

3 How should cyberspace be governed? Informal approaches: Norms, confidence- and capacity-building measures

Brokering global agreement on how to govern a domain as ubiquitous, convoluted and transformative as cyberspace is a formidable challenge. As discussed previously, cyber governance involves bringing together a range of stakeholders of unequal standing in terms of power and influence on the world stage, and attempting to reconcile fundamentally different views about the purpose and potential of this common resource. International treaties – a traditional means of governing global affairs – are one type of mechanism through which consensus may be forged. However, stakeholders are wary of codifying governance practices and processes in a comprehensive manner, concerned about how this may affect their economic interests and security. Moreover, once adopted, cyber treaties are likely to face "fatal implementation problems involving scope, compliance, and verification."[31] In such situations, informal approaches, which are based on current practice and leverage existing relationships, offer valuable opportunities for consensus-building and creating a template for effective, rules-based governance.

This section elaborates on three types of informal approaches to cyber governance: developing norms for responsible state behavior in cyberspace; confidence-building measures; and capacity-building measures. It should be noted at the outset that the current discussion on norm development and confidence- and capacity-building in cyberspace focuses largely on state actors. This does not imply that other stakeholders are unimportant; it simply reflects the political reality that "nation-states are still the most powerful actors internationally and we are seeing the steady, incremental expansion of sovereign control into cyberspace." This section will therefore focus primarily on state actors.

3.1 Developing norms for responsible state behavior in cyberspace

Norms can be defined as "shared expectations of proper behavior,"[33] and can be either affective (i.e. following custom and practice) or aspirational (i.e. seeking to shape current behavior).[34] Both types of norms can be observed at play in cyberspace. Cooperation within the technical community is often based on established practice, while both states and the private sector have sought to influence state behavior in cyberspace through initiatives such as the Global Conference on Cyberspace[35] and Microsoft's International Cyber Security Norms.[36] Norms can be addressed to both state and non-state actors. For example, the Global Commission on Internet Governance has proposed a Social Compact for Digital Privacy and Security "between citizens and their elected representatives, the judiciary, law enforcement and intelligence agencies, business, civil society and the Internet technical community."[37]
Norms can be difficult to crystallize and disseminate, but it is possible to identify three qualities that enable a norm to gain traction internationally: clarity, utility and do-ability.[38] Successful norms, therefore, are those that are organized around clear principles; demonstrate a

connection between norm-following and desired outcomes; and provide guidance on how to comply.[39]

There are several advantages to adopting a normative approach to governing cyberspace. Norms are not necessarily legally-binding, and are therefore less affected by the trust-deficit that can cripple attempts to negotiate, sign, and ratify international treaties.[40] The discourse on norms can also create a safe rhetorical space in which to discuss the different needs and values of stakeholders without creating explicit hierarchies.[41] This is particularly valuable, given that "the very essence of cyberspace holds different meanings among States with varying conceptions of the role of the State and the degree of sovereignty it may wish to assert."[42] Exploring what various stakeholders consider to be appropriate and responsible behavior in cyberspace provides an opportunity to create coalitions of like-minded actors who could agree broadly on the substance of a given norm. Consistent practice, even within a small group, can foster broader acceptance of a norm – for instance, through confidence- and capacity-building measures – which may ultimately result in a binding international agreement.

There are, however, some disadvantages to normative approaches. It has been argued that the discourse on norms is dominated by Western values and perspectives, and does not capture different imaginaries of cyberspace that exist elsewhere.[43] This, coupled with the rise of non-Western cyber powers like Brazil, India and China, underscores that in order to gain wide acceptance and legitimacy, norms will have to identify and articulate *global* values, rather than national or regional ones. Another disadvantage of governance through norms concerns the inability to influence the behavior of powerful state and non-state actors that can act unilaterally to undermine a free, open and secure cyberspace. While there may be a diplomatic cost to flouting widely upheld norms, this alone is unlikely to be an effective form of deterrence for determined actors.

It is also worthwhile considering what would constitute *progress* in norm development in cyberspace. Such progress can be measured along three axes: the number of stakeholders who accept a given norm; the degree of ambition in terms of the content of the norm; and the degree to which the norm is legally-binding (only this third feature relates directly to formal governance). Trade-offs exist between the three categories, which makes it difficult to achieve progress along all three axes simultaneously. For example, building consensus between a small number of states on norms that reflect the status quo, and doing so in the form of a non-binding, declaratory document is relatively easy. However, the more norms deviate from the status quo, and/or grow more legally-binding, the less likely it is that a significant number of stakeholders will subscribe to the norm. Movement along any of these axes could be considered progress, however, given the complex and dynamic nature of cyber governance.

The wide dissemination and institutionalization of norms does not happen automatically. In the domain of cyberspace, confidence- and capacity-building measures play an important role in promoting norms by fostering trust and cooperation between stakeholders and forging consensus on how to govern specific aspects of cyberspace. These measures are explored in greater detail below.

3.2 Confidence- and capacity-building measures in cyberspace

Confidence-building measures are not new to the realm of international relations. Such measures have long been used in areas such as arms control to mitigate uncertainty or mistrust, thereby preventing the escalation of conflict between states.[44] Confidence-building measures in cyberspace "work towards clarifying the parameters of States' perspectives and expectations in cyberspace through the sharing of national security frameworks, military doctrines, and other crisis-managements tools that could be useful in reducing uncertainty."[45]

The UN GGE and the Organization for Security and Cooperation in Europe (OSCE) have both articulated a range of concrete confidence-building measures for cyberspace, which include "exchanges of information on national [cyber security] strategies, organizations … and decision-making processes, sharing of ICT security incidents, and mechanisms for cooperation amongst law enforcement communities," as well as holding regular consultations, sharing best practices, and instituting national legislation to facilitate bilateral cooperation.[46]

It is clear that confidence-building in cyberspace focuses heavily on the area of cyber security. This makes sense, as it allows states to build on the cooperation that already exists between technical and law enforcement communities in order to tackle thornier issues, such as national security. It also highlights how cooperation on specific issues or sectors can be expanded to address more complex issues, once the requisite trust has been built. This provides support for the argument advanced in the previous section of this brief in favor of adopting an incremental, sectoral approach to negotiating international agreements.

Capacity-building is a less obvious, but no less important means of creating consensus on a range of cyber issues. As defined by the United Nations, capacity-building is meant to "invent, develop and maintain institutions and organizations that are capable of learning and bringing about their own continuing transformation, so that they can better play a dynamic role to sustain national development processes."[47] While cyber capacity-building efforts may at first glance appear to be little more than technical assistance, they can be "foreign policy tool[s] used to advance national interests … and norms," thus achieving "deep societal and political transformation."[48]

The Council of Europe's efforts to assist countries in the implementation of the Budapest Convention – for instance, through making local legislation fully compliant with the Convention and European data protection standards – provides an example of how capacity-building can be a vehicle for promoting particular values and norms of behavior in cyberspace.[49] Similarly, the ITU provides capacity-building assistance aimed at harmonizing the legal and regulatory frameworks for electronic communications in recipient countries.[50] Finally, the Global Forum on Cyber Expertise – a capacity-building platform launched during the 2015 Global Conference on Cyberspace – has the explicit goal of undertaking efforts that are consistent with international legal frameworks (e.g. UDHR, ICCPR, UN Guiding Principles on Business and Human Rights) and a multistakeholder model of governance.[51]

While capacity-building can be an effective and strategic means of ensuring that different stakeholders adhere to specific standards of behavior in cyberspace, it is important that such efforts are not coopted by powerful actors with narrow interests. Capacity-building should ultimately enable all stakeholders – donors and recipients – to access and utilize cyberspace on an equal footing by brokering genuine agreement on how this is best achieved. Such efforts should therefore combine top-down and bottom-up processes, and reflect the actual needs of recipient countries as well as the shared values of donors

and recipients.

The discussion in this section gives rise to three policy recommendations, which have implications for global governance beyond the domain of cyberspace:

- **Norms are useful for building trust and consensus in situations where states remain reluctant to make legally-binding commitments. Norms should be clear, useful and do-able to gain traction, and should strive to articulate global values.**
- **The dissemination and institutionalization of norms should be supported by confidence-building measures that seek to build on existing cooperation, and expand cooperation to more difficult issues once trust has been built.**
- **Capacity-building can be an effective and strategic means of promoting core values and standards of behavior in cyberspace. These efforts should safeguard the interests of both donor and recipient countries and preserve a free, open and secure cyberspace.**

Conclusion

This policy brief focused on how to make cyber governance more effective, and extrapolated general lessons for effective global governance. Three sets of recommendations emerge from this analysis, and can be summarized as follows:

- **Multistakeholder** models of governance can empower non-state actors to participate in the development and implementation of international public policy. The representativeness and effectiveness of multistakeholder governance models can be improved by greater transparency of decision-making procedures, including a prohibition on the use of vetoes; dedicating financial resources to enable disadvantaged stakeholders to participate in governance processes in a meaningful way; and allocating leadership positions in an equitable manner.
- **Formal arrangements**, in particular international treaty-making, are an important means of global governance. Policymakers should make full use of the flexibility provided by international law to create viable coalitions of states willing to adopt international agreements on specific themes. These agreements may serve as stepping stones towards as a comprehensive treaty in the long-term. Such an approach bolsters the rule of law in cyberspace and strengthens the credibility and relevance of international law in governing dynamic, multistakeholder-driven domains.
- Recognizing the limits of formal legal approaches, the brief underscores the need for **informal approaches** to global governance, which include developing and advancing norms that are clear, useful and do-able in order to build trust and consensus reflective of global values. Confidence-building measures can support the dissemination and institutionalization of these norms by building on existing forms of cooperation, and expanding cooperation to more difficult issues once trust has been built. Capacity-building is an effective and strategic means of promoting core values and standards of behavior in cyberspace, and should safeguard the interests of both donor and recipient countries.

Many important questions remain about how to improve the effectiveness of current processes and mechanisms of global governance, both within the area of cyber governance and beyond. With regard to multistakeholderism, how can we ensure that the contributions of non-state actors to global governance go beyond tokenism and have an actual impact on the development and implementation of global public policy? How can political realities and state interests be balanced with the need for full transparency and accountability in governance? Is it possible to

delineate clear roles for the private sector, civil society, international organizations and states in global governance, and if so, what are those roles? These questions are salient not only in the context of cyber governance, but also in other governance domains such as climate, oceans, and fragile states.

In terms of formal approaches to global governance, their success will likely be determined by the ability to enforce and monitor compliance with legally-binding international commitments. But who has the authority, legitimacy, and capabilities required to do so successfully on a global scale? This is a matter that must be resolved in order to respond effectively to a broad range of global challenges such as protecting human rights and establishing international environmental and labour standards.

Lastly, informal approaches circumvent many of the challenges formal approaches entail, but rely on voluntary compliance by stakeholders. How should we contend with powerful actors who do not comply voluntarily and eschew the values and principles upon which consensus has been built? Constraining self-interested policies and behavior on the part of powerful actors such as states, multinational corporations and interest groups remains a challenge not only in cyberspace, but for global governance more generally. The subsequent phases of the Global Governance Reform Initiative (GGRI) will strive to answer these and other questions by examining how global governance works in other challenging domains.

Endnotes

1 | Laura DeNardis, *The Global War for Internet Governance* (New Haven and London: Yale University Press, 2014) 227.

2 | *Ibid, 226.*

3 | *Ibid, 227.*

4 | Milton Mueller and Ben Wagner, "Finding a Formula for Brazil: Representation and Legitimacy in Internet Governance," Internet Policy Observatory, 8, accessed August 11, 2015, http://www.internetgovernance.org/wordpress/wp-content/uploads/MiltonBenWPdraft_Final_clean2.pdf

5 | Alejandro Pisanty, "Empowerment of non-governmental actors from outside the United States in multistakeholder Internet governance," (Working Paper for the Global Governance Reform Initiative Project of The Hague Institute for Global Justice, 2015) 25.

6 | Milton Mueller, Networks and States: *The Global Politics of Internet Governance* (Cambridge: MIT Press, 2010) 248.

7 | *Ibid, 248.*

8 | Enrico Calandro and Nicolo Zingales, "Stakeholders' involvement and participation in the Internet governance ecosystem from an African perspective," (Working Paper for the Global Governance Reform Initiative Project of The Hague Institute for Global Justice, 2015) 10.

9 | Alejandro Pisanty, "Empowerment of non-governmental actors," 7.

10 | Bertrand de la Chapelle, "The Internet Governance Forum: How a United Nations summit produced a new governance paradigm for the Internet age," in *Governing the Internet: Freedom and Regulation in the OSCE Region*, eds. Christian Moeller and Arnaud Amouroux (OSCE, 2007) 26.

11 | Internet Governance Forum Brochure, accessed August 11, 2015, http://intgovforum.org/cms/2014/IGFBrochure.pdf

12 | "Chair's Statement," Global Conference on Cyberspace, accessed August 10, 2015, https://www.gccs2015.com/sites/default/files/documents/Chairs%20Statement%20GCCS2015%20-%2017%20April.pdf

13 | Mueller and Wagner, "Finding a Formula for Brazil," 9.

14 | Bart Cammaerts, "Power dynamics in multi-stakeholder policy processes and intra-civil society networking," in *The Handbook of Global Media and Communication Policy*, eds. Robin Mansell and Mark Raboy (Malden, MA: Wiley-Blackwell, 2011) 8.

15 | "NETmundial Multistakeholder Statement," Global Multistakeholder Meeting on the Future of Internet Governance, accessed August 11, 2015, http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf

16 | "Statement on NETmundial," Association for Progressive Communications, accessed August 11, 2015, https://www.apc.org/en/node/19224

17 | Bart Cammaerts, "Civil society participation in multistakeholder processes. Between realism and utopia" in Making Our Media. Global Initiatives toward a Democratic Public Sphere. Volume Two: National and *Global Movements for Democratic Communication,* eds. Laura Stein, Dorothy Kidd and Clemencia Rodriguez (Cresskill, NJ: Hampton Press, 2009) 90.

18 | Stefania Milan, "Civil Society Participation Beyond Smoke and Mirrors: An Assessment of Multi-Stakeholder Mechanisms in Cyberspace Governance," (Working Paper for the Global Governance Reform Initiative Project of The Hague Institute for Global Justice, 2015) 5.

19 | *Ibid, 6.*

20 | Bart Cammaerts and Nico Carpentier, "The unbearable lightness of full participation in a global context: WSIS and civil society participation," in *Towards a Sustainable Information Society: Beyond WSIS,* eds. Jan Servaes and Nico Carpentier (Bristol and Portland: Intellect, 2004) 20.

21 | "NETmundial Closing Session," Global Multistakeholder Meeting on the Future of Internet Governance, accessed August 11, 2015, http://netmundial.br/wp-content/uploads/2014/04/NETMundial-23April2014-Closing-Session-en.pdf

22 | Calandro and Zingales, "Stakeholders' involvement and participation," 12.

23 | Milan, "Civil Society Participation Beyond Smoke and Mirrors," 3.

24 | *Ibid,* 5.

25 | "Chair's Statement," 1.

26 | The Budapest Convention, signed in 2001 and in force since 2004, commits mostly European and a number of other states to mutual legal cooperation with regard to specific crimes committed in cyberspace such as the dissemination of child pornography, large-scale copyright infringement and online fraud. *Convention on Cybercrime*, Budapest, 23 November 2001, Council of Europe Treaty Office CETS No. 185, accessed August 10, 2015, http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

27 | United Nations, General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98 (24 June 2013) 2.

28 | "Chair's Statement," 9.

29 | Vienna Convention on the Law of Treaties, Vienna, 23 May 1969, *United Nations Treaty Series*, vol. 1155, p. 331, accessed August 10, 2015, http://legal.un.org/ilc/texts/instruments/english/conventions/1_1_1969.pdf. Though some important powers such as India and the United States have not ratified the Convention, most of its content represents customary international law.

30 | While negotiations for a Comprehensive Convention on International Terrorism remain deadlocked, there exist today 15 counter-terrorism international conventions, which have entered into force and cover specific issues such as acts committed on board aircrafts or the suppression of the financing of terrorism.

31 | James Lewis, "Liberty, Equality, Connectivity: Transatlantic Cybersecurity Norms," *Center for Strategic & International Studies*, February 2014, 4.

32 | *Ibid, 2.*

33 | Martha Finnemore, "Cultivating International Cyber Norms," in *America's Cyber Future: Security and Prosperity in the Information Age,* eds. Kristin Lord and Travis Sharp (Washington: Center for a New American Security, 2011) 90.

34 | The Hague Institute for Global Justice, "Final Report," Report on Official Side-Events Co-Organized by The Hague Institute for Global Justice and The Observer Research Foundation for the 2015 Global Conference on Cyberspace (GCCS), 15 April 2015.

35 | Global Conference on Cyberspace 2015, accessed August 10, 2015, https://www.gccs2015.com/

36 | Microsoft, *International Cyber Security Norms:*

Reducing Conflict in an Interdependent World (December 2014).

37 | "Toward a Social Compact for Digital Privacy and Security," Statement by the Global Commission on Internet Governance, 1, accessed August 28, 2015, https://ourinternet-files.s3.amazonaws.com/publications/GCIG_Social_Compact.pdf

38 | Finnemore, "Cultivating International Cyber Norms," 91-92.

39 | *Ibid.*

40 | Lewis, "Liberty, Equality, Connectivity," 3.

41 | The Hague Institute, "Final Report," comments by Prof. Ivan Arreguín-Toft.

42 | Chelsey Slack, "Wired Yet Disconnected: The Governance of Internet Cyber Relations," (Working Paper for the Global Governance Reform Initiative Project of The Hague Institute for Global Justice, 2015).

43 | The Hague Institute, "Final Report," comments by Dr. Alison Gillwald.

44 | Slack, "Wired Yet Disconnected," 10.

45 | *Ibid.*

46 | *Ibid,* 10-11.

47 | United Nations, *United Nations System Support for Capacity-building*, E/2002/58 (14 May 2002) 4; see also Patryk Pawlak, "Capacity-building in Cyberspace as an Instrument of Foreign Policy," (Working Paper for the Global Governance Reform Initiative Project of The Hague Institute for Global Justice, 2015) 2.

48 | Pawlak, "Capacity-building in Cyberspace," 1-2.

49 | *Ibid*, 6-8.

50 | *Ibid,* 11.

51 | "Hague Declaration on the GFCE," Global Conference on Cyberspace, accessed August 10, 2015, https://www.gccs2015.com/sites/default/files/documents/The%20Hague%20Declaration%20on%20the%20GFCE.pdf

The Hague Institute
for Global Justice

Sophialaan 10, 2514 JR The Hague, The Netherlands
t +31 (0)70 30 28 130 | e info@TheHagueInstitute.org | @HagueInstitute
w TheHagueInstitute.org