AN ANALYTICAL REVIEW AND COMPARISON OF OPERATIVE MEASURES INCLUDED IN CYBER DIPLOMATIC INITIATIVES

Deborah Housen-Couriel, *Adv., LL.M., MPA-MC*

BRIEFING №2

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This Brief focuses on the analytical gaps with respect to the incorporation of measures into 84 contemporary cyber diplomatic initiatives; and the opportunities these gaps present for bolstering global cybersecurity and IPS of cyberspace. The initiatives studied are presented in Figure 1, and the accompanying analytical matrix is included in Appendix 1. Each initiative is categorized according to the type of initiating stakeholder, be it a state, international organization, intergovernmental group, non-governmental organization, academia, industry or private sector actor, law enforcement authority or other entity. Thus, in broadening the usual understanding of the term "diplomatic initiative", non-state initiatives have been included in the analysis to the extent that a reasonable basis for comparison and analysis was present. Initiatives that cross stakeholder boundaries at this first stage are relatively rare, and have been so noted in the analysis.

In the initiatives studied, 40 distinct operative measures have been identified and grouped for analysis into 27 topic clusters (for example, "Information sharing measures" and "Legislation, mutual legal assistance and legal training"). The topic clusters were not predetermined, but rather emerged from the research and analysis of the documents reviewed.

Key findings of the research include a listing of measures that are most commonly included in diplomatic initiatives across stakeholder groups. Moreover, the analysis revealed a "convergence of concept" around certain measures which different types of stakeholders have incorporated into initiatives. These are: information sharing in general, sharing of information around cyber threats, law enforcement cooperation, protection of critical infrastructure, mechanisms for cooperation with the private sector and civil society, arrangements for international cooperation, a mechanism for vulnerability disclosure, regular dialogue, the mandating of general legislative measures, training of cyber personnel, cyber education programs and conducting exercises and tabletops.

Additional analysis is required to elucidate whether the frequency of incorporation of these measures is due to their independent adoption in a variety of initiatives, or to redundancy in initiatives among similar stakeholders. Nonetheless, we propose in this Brief that this convergence of concept does indicate progress in the elucidation of the potential zones of agreement around measures for bolstering cybersecurity and at the international level.

The next stage of mapping, comparison and analysis for the development of global and national public policy with respect to IPS of cyberspace should address questions such as (a) the comparison of new initiatives to more mature ones; and (b) overlap or redundancy in stakeholders' incorporation of measures vs. cumulative and complementary take-up. Finally, to the end of influencing and leveraging future cyber diplomatic initiatives, a model for identifying proxies for impact and success of measures would deepen the understanding of which measures should be prioritized in public policy efforts.

SECTION 1: INTRODUCTION AND INITIAL FINDINGS RESULTING FROM THE GAP ANALYSIS OF CYBER DIPLOMATIC INITIATIVES

1.1 FRAMING THE NORMATIVE CHALLENGE

Diplomatic initiatives to advance global levels of cybersecurity have accelerated significantly over the past five years,[69] reflecting two key trends. The first is a deepened understanding on the part of decisionmakers that there is a steady increase in the vulnerabilities of national and trans-national computer systems and information assets to hostile acts in cyberspace. The second is the recognition that development of normative frameworks to govern state and non-state actor activity in cyberspace has become a critical issue at the global level, whether advanced by state or non-state actors.[70] A recent study has described this normative challenge as "one of the most pressing problems of global governance."[71]

The range of traditional legal and policy tools for development of such frameworks have included treaties, codes of conduct, agreements, memoranda, public declarations, national policies and the like: instruments that set transparent expectations and standards for responsible behavior of actors on the international plane and permit others to assess their intentions and actions. In the best of cases, it has been possible to conclude formal treaties that are binding on state signatories and inform policy and decision-making processes, as with the 2001 Council of Europe Convention on Cybercrime.[72] Despite criticism of the Convention at the level of its implementation and enforcement, it has been effective in instituting common definitions of cyber-enabled criminal activity among its 56 state signatories and influencing such definitions in some regional treaties.[73]

---

[69] Of the 84 initiatives identified and analyzed in this Brief, 70 (83%) date from 2012 to the present.

[70] The normative challenges in this context have been explored by several scholars. See, for example, Kubo Macak, *From Cyber Norms to Cyber Rules: Re-engaging States as Lawmakers*, Leiden Journal of International Law, Vol. 30 (December 2017), pp. 877-899; and Martha Finnemore and Duncan B. Hollis, *Constructing Norms for Global Cybersecurity*, American Journal of International Law, Vol. 110, No. 3 (July 2016), pp. 425- 479; and Michael Schmitt, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical Vade Mecum*, Harvard Law School National Security Journal, Vol. 8, Issue 2 (2017).

[71] Finnemore and Hollis, *ibid*, at 429.

[72] Council of Europe, Convention on Cybercrime, ETS No.185, 2001.

[73] See, for instance, the African Union Convention on Cyber Security and Personal Data Protection, Article 29 and the Arab League Arab Convention on Combating Information Technology Offences, Articles 6-9.

Nonetheless, reaching formal agreement on binding norms governing conduct in cyberspace has proven difficult.[74] Beyond the challenges caused by the present fragmented international system and the political gaps that divide state and organizational actors,[75] cyberspace is presently characterized by several factors that impede the evolution of such binding norms. These include (a) rapid technological developments that introduce new individual and organizational activities in cyberspace, such as the Internet of Things;[76] (b) state and organizational behaviors that continue to lack transparency; (c) attribution challenges; (d) controversy about content online; and (e) the unprecedented uses and influences of social media. The widening gap between the need for normative clarity in cyberspace, on the one hand; and the possibilities of achieving consensus or agreement around norms, on the other, has changed expectations around what is achievable. This is due to both a lack of normative consensus among stakeholders and uncertainty around the current feasibility of such an undertaking at the global level.[77]

Thus, for example, the 2015 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security - the last consensus report of the GGE Group - advocated "voluntary, non-binding norms of responsible State behavior" as a means to reduce risks to international peace, security and stability in cyberspace.[78] Moreover, specific measures, tools, methodologies and best practices that expressly avoid normative determinations and controversies may at present be more relevant to actors' national and global cybersecurity needs and requirements, given the present difficulties with achieving broad agreement around substantive norms.[79] Such measures, including CBMs, are of course not disconnected from normative implications - in fact, some actors explicitly attribute a normative dimension to them[80] - and may have important *de facto* effects that move the long-term normative process forward.[81] This proposition is supported by the initial results of the gap analysis of 84 initiatives conducted for the present Brief.[82]

---

[74] See James Lewis, *Sustaining Progress in International Negotiations on Cybersecurity, Center for Strategic and International Studies*, July 2017, p.4: "The dynamics of fragmentation in the international system limit the scope for global norms development." The challenges to achieving geopolitical agreement even around issues that diplomatic actors fully agree are beyond the scope of this Brief.

[75] See Alex Grisby, *Overview of Cyber Diplomatic Initiatives*, GCSC, November 2017.

[76] Pew Research Center, *The Internet of Things Will Thrive by 2025*, May 2014.

[77] See references at note 2.

[78] A/70/174, 22 July 2015, at p. 7, < http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174>.

[79] The 2011 definition of cybersecurity in the framework of the non-binding standard of the International Telecommunication Union, ITU-T X.1500 ("Overview of cybersecurity") is notable in this context of normative neutrality. Cybersecurity is there defined, in part, as "The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets."

[80] See, for example, European Union Parliament, *Briefing: Cyber diplomacy confidence building measures*, October 2015. There, CBMs are categorized as part of the normative project, either as support structures for norm implementation or autonomously.

[81] In fact, there are varying understandings of the terminology used by the GGE and other bodies, and the degree to which CBMs are normative or procedural in nature. "The discussion about confidence-building measures in cyberspace is closely linked to the parallel debates about acceptable norms of state behaviour. While the focus on norms, both in the existing international law and non-binding political agreements, helps to establish international level of expectations about states' behaviour in cyberspace, development of CBMs provides practical tools to manage these expectations" (Patryk Pawlak, *Confidence Building Measures in Cyberspace: Current Debates and Trends*, in in Anna-Maria Osula and Henry Rõigas (Eds.), International Cyber Norms: Legal, Policy & Industry Perspectives, CCDCOE, 2016, pp.129– 153, at p. 133.)

[82] Three additional initiatives have been recently added to the analysis and remain to be will be fully integrated.

1.2 METHODOLOGY

This study is based on a literature review[83] and analysis of publicly-available primary sources. While the listing of initiatives in Figure 1 does not claim to constitute a comprehensive listing of all contemporary cybersecurity-related initiatives, it aims to include a broad range of initiators and stakeholders such as standards bodies, law enforcement entities, NGOs and private sector organizations. The aim of this inclusive approach is to reflect the challenges posed by increasing diversity of international actors and to better draw out elements of commonality among current initiatives. Thus, the critical question posed regarding the inclusion or non-inclusion of a given initiative was the degree to which it incorporates measures, whether binding or voluntary, in addressing the IPS of cyberspace.

Nonetheless, the present scope did not permit an analysis of whether the frequency with which such measures are incorporated into several initiatives is due to redundancy and overlap (i.e., the same stakeholders incorporating it in several initiatives); or cumulative (i.e., reinforced in the initiatives of different stakeholders). This is an important methodological distinction in weighing the actual commonality of a given measure, and should be explored in further research and through the development of corresponding mapping tools.[84] Likewise, the actual impact of a measure on the practice of state and non-state actors and proxy measurements for its success in bolstering cybersecurity is a critical issue for policy development, as pointed out by scholars and other commentators, yet these remain at present open issues for further study.

The categorization and analysis of the 84 cyber diplomatic initiatives could have been approached from several perspectives. This Brief classifies initiatives by the type of initiating stakeholder (i.e., regional organization, law enforcement entity). The cross-reference of measures stemmed organically from the research, through comparison and analysis of the documents studied.

Finally, we note that the terms "operative measures" or "measures", as used in this Brief, refer collectively to those operative elements included in initiatives that may be designated as best practices, guidelines, recommendations, frameworks, or confidence building measures (CBM's). The current usage of these terms on the part of stakeholders is fluid, and, as discussed above, are likely to incorporate normative dimensions.[85]

Additional methodological challenges, limitations of scope and topics for further research are detailed in Part II below.

1.3 INITIAL FINDINGS OF THE GAP ANALYSIS

COMMON OPERATIVE MEASURES

The gap analysis that will be further elaborated herein revealed that the following operative measures are included in **more than 25% of the total cyber diplomatic initiatives** (21 out of the total 84). They are, in order of the frequency of their inclusion:[86]

Information sharing measures in general

---

[83] Selected sources are included following Part V in the full version of the Brief.

[84] Nevertheless, Figure 1 contains the detailed data for *prima facie* evaluation of the degree of redundancy.

[85] See the discussion on this point in Finnemore and Hollis, note 2.

[86] The implications of the "frequency of inclusion" parameter are discussed in Section II below in the review of methodology. In general, it is difficult within the current scope of research to specify whether frequency of inclusion is redundant or cumulative, and this issue has been noted as a topic for further research.

- Exchange between stakeholders of information about strategies, policies, legislation, best practices, and cyber infrastructure capacity building

Mechanisms for international cooperation

- Cyber diplomacy projects, convening of conferences, task forces, learning exchanges, professional study sessions, dedicated websites

Mechanisms for government - private sector cooperation

- Closed industry roundtables convened by regulators, Information Sharing and Analysis Centers (ISACs), regulatory protections for the sharing of sensitive data between the private sector and the government and among private actors

Specific measures for transnational law enforcement cooperation and mutual legal assistance for cybercrime

- Agreed forensics procedures, standardized exchange of breach data in a timely manner, joint training of law enforcement officers, ongoing communications among cyber units in national police forces

Establishment of a specific national or organizational point of contact for information exchange

- Including a specific mandate or mention of points of contact established as CERTs, CSIRTs and FIRSTs

Technical standards are recommended or required

- Such as the ISO 27001 information technology security techniques series or the NIST Cybersecurity Framework

Creating a culture of cybersecurity or information security

- Through nationwide educational programs, advertising campaigns, transparency around legal and regulatory initiatives and platforms for public input into these

"Regular dialogue"

- Ongoing, regularly scheduled regional and bilateral meetings that address both a permanent common agenda and current issues. Such meetings may take place as "Track 2" and "Track 3" dialogues, as well

Threat sharing (in general)

- Although often not transparent, threat sharing mechanisms may include public and private actors, as well as national security entities

Mechanisms for government - third sector cooperation (NGO's, academia, civil society, informal groups)

- Government financial support for NGO participation in international *fora*, investment in academic research programs and university degrees supporting cybersecurity, support for government outreach to the public through civil society activities for cybersecurity awareness and training

Developing common terminology

- Definition of cybercrimes at the level of formal agreements such as the Cybercrime Convention, cooperation on common terminology through standards bodies, glossaries collated through academic and professional joint efforts

Additional key findings are detailed in Part III.

MAPPING OF NORMATIVE ELEMENTS

Parallel to the analysis of the operative measures that are at the core of this Brief, normative elements have also been identified for each initiative and mapped out on a separate matrix, included in Appendix 2. This was done for the sake of completeness of the research, as there is significant overlap between operative and normative elements in several instances.[87] One example is Measure #6, "Ensuring technical interoperability of networks", which is ostensibly a technical task, yet has normative implications for global internet governance. Another is Norm #34 governing "the responsibility to report ICT vulnerabilities", which necessitates a technically-safe reporting mechanism. The solution to these overlaps was to include both measures and norms in the analysis, allowing some flexibility in their characterization.

Nevertheless, the core analysis of the Briefing remains focused on measures although some comparisons between the analysis of measures and norms have been addressed. Thus, the following normative elements were incorporated in more than 25% of the total cyber diplomatic initiatives (21 out of the total 84, see Appendix 2):[88]

1. Human rights, civil rights, and/or individual rights should be respected in cyberspace
2. Norms relating to internet/cyberspace governance in general
3. Protection of personal and private data
4. Norms specifying international cooperation

It is interesting to note, even from these two initial lists, that significantly more measures than norms (11 v. 4) are incorporated in the initiatives at the cutoff point of a 25% of the initiatives. This point will be further elaborated herein.

[87] Pawlak, note 13.

[88] See the explanation and reservations regarding the frequency parameter in note 18.

SECTION 2: SCOPE OF THE WORK, METHODOLOGY AND ISSUES FOR FUTURE RESEARCH

2.1 SCOPE

The Brief takes a broad and inclusive approach to the type of cyber diplomatic initiative included, by including a range of modes of agreement on operative measures. These include multilateral treaties and draft agreements (such as the Shanghai Cooperation Organization's Agreement on Cooperation in the Field of Information Security[89]); as well as less formal modes such as industry initiatives (including Microsoft's proposal for the establishment of an International Cyberattack Attribution Organization[90] and the CPMI-IOSC's Guidance on cyber resilience for financial market infrastructures[91]). In addition, some of the initiatives reviewed were not "international" by original intent, but have become so because of the degree of their *de facto* adoption by cyberspace actors in many states and organizations, such as the NIST Cybersecurity Framework.[92] The aim of this inclusive approach is to reflect the challenges posed by increasing diversity of international actors and, as discussed above, to better draw out elements of commonality among current initiatives. In sum, the critical question posed regarding the inclusion or non-inclusion of a given initiative was the degree to which it incorporates measures, whether binding or voluntary, in addressing the IPS of cyberspace.

The scope of the research, as originally prescribed, does not include evaluation of the actual impact of measures on cybersecurity policy, proxy parameters for evaluating their success, nor policy recommendations, although these are touched upon in the concluding Part V.

2.2 WORKING DEFINITION OF "CYBER DIPLOMATIC INITIATIVE"

We have used "cyber diplomatic initiative" to refer to any initiative that incorporates measures that are intended to boost cybersecurity on the international plane. The flexibility of this approach enables the inclusion of sources such as voluntary frameworks and measures, proposals from policy and academic experts, and industry guidelines, as explained above in Part I. The categorization by type of stakeholder may allow some conclusions to be drawn about the potential impact of each initiative on global cybersecurity. For instance, Initiative #3, the Additional Protocol to the

[89] The most recent version is available at https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreement.pdf.

[90] See Microsoft, *Establishing an International Cyberattack Attribution Organization to strengthen trust online*, no date.

[91] Committee on Payments and Market Infrastructures Board of the International Organization of Securities Commissions, Guidance on cyber resilience for financial market infrastructures, June 2016.

[92] The NIST Framework was developed in response to Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," on February 12, 2013 but see (regarding extensive international adoption) Evan D. Wolff, *The Global Uptake of the NIST Cybersecurity Framework*, February 2016.

Council of Europe Cybercrime Convention,[93] has the potential to impact signatory state behavior on the international plane differently from Initiative #63, the Oxford Global Cyber Security Capacity Centre's Cybersecurity Capacity Maturity Model for Nations. Yet as illustrated by the example of measure #4.8 for the establishment of cyber hotlines connecting the US, Russia and China (as well as MERIDIAN members[94]), caution should be exercised in drawing any definitive conclusions about the comparative impact of measures and norms based on the type of initiative or the stakeholders involved, in terms of effective compliance and overall impact on cybersecurity.[95]

METHODOLOGICAL CHALLENGES AND SCOPE LIMITATIONS

The listing of initiatives in Figure 1 has aimed to encompass all contemporary cybersecurity-related initiatives, yet does not claim to be comprehensive. Even during the Brief's drafting process several new initiatives were published. Due to limitations of time and scope it does not include, for instance, e-commerce frameworks. Several regimes relating to the protection of personal data have been included, however, because of their cybersecurity relevance.[96]

Three methodological challenges are a cause for caution in assessing the results of the gap analysis. The first concerns (a) the difficulty in accessing important initiatives, especially from Asian countries, either because they are not transparent online or because of language barriers.[97] This point has substantive implications regarding the measures and norms that are incorporated in the analysis and excluded from it, a limitation which will be discussed in the Conclusion. The second is (b) the overlapping nature of some measures, which may cause inconsistency in their categorization.[98] Finally, assessing measures by quantifying the degree of their inclusion in initiatives only provides part of the overall cybersecurity picture. One example is the inclusion of measure #4.8 "Cyber hotline for issues that may escalate" by only five initiatives out of the 84. Yet (c) the contribution of this single measure to global cybersecurity may be much greater than the inclusion of, for instance, measure #15 "Creating a culture of cybersecurity or information security", incorporated by 25 initiatives.

ISSUES FOR FUTURE RESEARCH AND POLICY DEVELOPMENT THAT ARE BEYOND SCOPE

The research gave rise to some additional questions which are beyond the scope of this Brief, yet need attention to further the comparative analysis presented here. These include (a) initiatives addressing e-commerce; (b) the degree to which initiatives are implemented and enforced; (c) even when fully enforced - determination of their actual impact on

---

[93] Council of Europe, Additional Protocol to the Cybercrime Convention, ETS 189, 28 January 2003.

[94] A cyber hotline is also included in the OSCE measures (Decision 1202, 2016, #8).

[95] On this point, one international law scholar has observed: "Some non-obligatory international norms have produced important results, managing to obtain voluntary compliance, and even exceeding the original expectations of their supporters [...] International law tends to be effective whenever compliance is more or less automatic. This can happen either because there is no significant incentive to violate what has been agreed upon or there are reciprocal gains achieved by maintaining reliable standards." (Richard Falk, "'Voluntary' International Law and the Paris Agreement", *Global Justice in the 21st Century*, January 16, 2016),

[96] The EU General Data Protection Regulation, the African Union Convention on Cybersecurity and Personal Data Protection, and the APEC Privacy Framework have been included.

[97] One important example is China's recent regulatory initiative on cybersecurity and data protection. See Sara Xia, China Cybersecurity and Data Protection Laws: Change is Coming, China Law Blog, May 10, 2017.

[98] For instance, Norm #3 "Protection of CERTs and other cyber emergency responders" may be viewed by some as a measure without normative content. However, its grouping together with normative content in some initiatives determined its inclusion in the norms matrix.

cybersecurity; (d) measures that are relatively overlooked, such as research and development programs and security and privacy by design; and (e) sources of funding for the initiatives, their costs, and their financial sustainability. In addition, the data collected might be utilized to explore other research directions, including chronological patterns, the types of norms or measures preferred by a type of stakeholder, and the degree of cross-referencing among initiatives. The next stage of mapping, comparison and analysis for the development of global and national public policy with respect to cybersecurity and the IPS of cyberspace should address questions such as the comparison of new initiatives to more mature ones and overlap in stakeholders' incorporation of measures vs. cumulative and complementary take-up. A model for identifying proxies for impact and success of measures would deepen the understanding of which measures should be prioritized in public policy efforts.

SECTION 3: KEY FINDINGS WITH RESPECT TO CLASSIFICATION OF CYBER DIPLOMATIC INITIATIVES ACCORDING TO TYPE OF STAKEHOLDER

Figure 1 lists the initiatives reviewed and analyzed for this Brief.[99] We preface it with some key findings with respect to the types of stakeholders engaged with diplomatic cyber initiatives.

1. Consistent with the assumptions reviewed Part I above, **few multilateral treaties have so far been concluded to deal with cyber security**. Of the five included here, the SCO Code of Conduct (6 state parties) and the CoE Convention on Cybercrime (56 state parties) are the two core initiatives for cybersecurity. The ITU basic instruments (193 state parties) deal with the global governance of cyberspace infrastructure and some technical aspects of global communications, and the WTO GATS Agreement on Telecommunications (88 state parties) has only recently been linked to a cybersecurity context.[100] The multilaterals are strong on the adoption of measures promoting common cybersecurity terminology (#3); information sharing in general (#4.1); closing the digital divide (#18); common definitions of cybercrimes (#5.2); law enforcement cooperation (#5.3); and adoption of standards (#6).
2. There are **20 initiatives of regional organizations** – 24 when the OSCE 2016 initiatives are included (they have been separated out to highlight the organization's work on CBMs). This group of initiatives includes most regions of the world, and a robust range of measures, including vulnerability disclosure (in the EU /ENISA Good Practice Guide on Vulnerability Disclosure);[101] a strong level of incorporation of information sharing methods, including real-time, 24/7 sharing (#4.4); adoption of standards (#6); law enforcement cooperation (#5.3); R&D (#20) and mechanisms for governmental cooperation with the private and third sectors (#'s 9 and 10).

[99] There are some anomalies in the listing worth noting: the International Telecommunication Union's treaty documents appear under multilateral arrangements, while a resolution from that organization's plenipotentiary conference appears under the designation of Specialized Agency Conferences. The Wassenaar Arrangement is not categorized as a multilateral agreement as it is not considered a formal treaty by participants.

[100] See Chris Mirasola, U.S. Criticism of China's Cybersecurity Law and the Nexus of Data Privacy and Trade Law, Lawfare (blog), October 10.2017.

[101] ENISA, *Good Practice Guide on Vulnerability Disclosure*, January 2016.

3. At least four countries have published self-proclaimed "international" cybersecurity strategies: the US (2011), China (2017), the Netherlands (2017) and Australia (2017). Three out of the four have unanimously incorporated measures for law enforcement cooperation (#5.3) and general international sharing (#4.1). Other measures adopted by them include supply chain supervision (#12), threat sharing (#4.3), private sector engagement (#9) and technical standards (#6).[102]
4. It is evident to all observers that private sector actors have begun to engage intensively with cybersecurity at the global level. They have proposed at least eight initiatives in the years 2016-2017. Leaving aside their engagement with normative issues that in the past were in the exclusive purview of states (Microsoft's From Articulation to Implementation: Enabling progress on cybersecurity norms and Digital Geneva Convention are the prime examples; and ICANN's Draft Framework for Registry Operator to Respond to Security Threats may carve out a much more activist role for the private sector in coping with hostile activity in cyberspace). Some of the measures included in private sector initiatives are the establishment of mechanisms for communicating vulnerability disclosures (#4.5), the use of ISACs and FIRSTs (#'s 4.7 and 4.8), Microsoft's concept of establishing global attribution mechanisms (#5.4), cooperation arrangements between governments and the private sector and B2B (#'s 9 and 11), supply chain supervision (#12) and development of risk assessment mechanisms for increasing cybersecurity (#22).

In concluding this summary of some key cyber measures according to type of initiative stakeholders, three final examples involving three different types of stakeholders are salient, and significant to the processes taking place in the incorporation of measures at the global level. The 2015 GGE Report, the 2016 OSCE initiatives on CBMs;[103] and the 2017 bilateral agreement between India and the US indicate many identical measures. The US - India agreement includes 20 distinct measures.[104] It shares seven of these with the GGE and OSCE initiatives: information sharing in general (#4.1), sharing of information around cyber threats (#4.3), law enforcement cooperation (#5.3), protection of critical infrastructure (8.2), mechanisms for cooperation with the private sector and civil society (#'s 9 and 10), and arrangements for international cooperation (#19). At least two of these three actors have in common six more measures: a mechanism for vulnerability disclosure (#4.5), regular dialogue (#4.6), the mandating of general legislative measures (#5.1), training of cyber personnel (#13), cyber education programs (#14) and conducting exercises and tabletops (#17).

This "convergence of concept" around several measures to which different types of stakeholders have shown themselves willing to incorporate into initiatives constitutes, we propose, progress in elucidating the potential zones of agreement for measures at the international level.

The initiatives reviewed and analyzed are presented in the following table. The key number for the measure as it appears in the analytical table in Appendix 1 is indicated in green.

[102] The Netherlands international strategy takes a slightly different approach.

[103] See the OSCE's *Efforts Related to Reducing the Risks of Conflict Stemming from the Use of ICTs* and Decision No. 1202 on Confidence-Building Measures.

[104] It would be interesting to compare this 2017 initiative with bilateral agreements concluded by each party with other countries, and to follow its use in the future as a possible template for a bilateral accord on measures.

Figure 1: DIPLOMATIC CYBER INITIATIVES BY STAKEHOLDER	Key (#) and Description *Initiatives are listed in reverse chronological order within each category.*	Year
STATE-TO-STATE Multilateral treaties		
	1Shanghai Cooperation Organization, International Code of Conduct for Information Security	2015
	2International Telecommunication Union, Constitution, Convention and Administrative Regulations (Radio Regulations and Telecom Regulations (Melbourne) (Dubai)	2014 (RR 2016, ITR 1988, 2012)
	3Council of Europe, Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems	2003
	4Council of Europe, Convention on Cybercrime	2001
	5WTO, General Agreement on Trade in Goods and Services (Annex on Telecommunications)	1997
Regional		
	6African Union, Internet Infrastructure Security Guidelines for Africa: A joint initiative of the Internet Society and the Commission of the African Union ("Recommendations")	2017
	7EU, Proposal for an EU Regulation on strengthening ENISA	2017
	8EU, Code of Conduct for Cloud Services Providers, v.1.7	2017
	9EU, Joint Communication, Resilience, Deterrence and Defence: Building strong cybersecurity for the EU	2017
	10 OAS, Inter-American Committee Against Terrorism, Working Group on Cooperation and Confidence-Building Measures in Cyberspace	2017
	11 ASEAN, Chairman's Statement (para's 23 and 32) and ASEAN Cyber Capacity Programme	2017
	12 Ibero-American General Secretariat, Special Communication on Cooperation	2016

	on Cybersecurity	
	13EU, Network Security Directive	2016
	14EU, General Protection of Data Regulation	2016
	15Council of Europe, Internet Governance - Council of Europe Strategy 2016-2019	2016
	16NATO, Warsaw Summit Communique re article 5 applicability in cyberspace	2016
	17 ASEAN, Regional Forum Work Plan on Security of and in the Use of ICTs	2015
	18APEC Telecommunications and Information Working Group Strategic Action Plan 2016-2020	2015
	19 APEC Cross Border Privacy Rules (CBPR) system and Privacy Framework	2015
	20EU/ENISA, Good Practice Guide on Vulnerability Disclosure	2015
	21African Union, Convention on Cyber Security and Personal Data Protection	2014
	22EU, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace	2013
	23League of Arab States/ Gulf Cooperation Council, Arab Convention on Combating Information Technology Offences	2010
	24UN Economic Commission for Africa , African Regional Action Plan on the Knowledge Economy (ARAPKE)	2005
	25OAS, Adoption of a Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: a Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity	2004
	26UN Economic Commission for Africa, African Information Society Initiative	1996
Bilateral		
	27 US-India	2017
	28China-EU cybersecurity agreements / Joint Summit 2012	2015
	29 China-Russia Information Security Agreement	2015
	30China-US Agreement	2015
	31 US- Russia	2015
	31.5 China-Japan-Korea Joint MoU on CSIRT with National Responsibility	2011
UNILATERAL STATE INITIATIVE WITH INTENT TO APPLY ON THE		

INTERNATIONAL PLANE		
	32China, International Strategy of Cooperation on Cyberspace	2017
	32.1 Netherlands Building Digital Bridges- International Cyber Strategy	2017
	33 Australia, International Cyber Engagement Strategy	2017
	34US, International Strategy for Cyberspace	2011
INTERNATIONAL ORGANIZATIONS United Nations Security Council, General Assembly and GGE		
	35Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE)	2015
	36 Security Council Resolution 2178 (pp. 2-3)	2014
	37GGE 2013	2013
	38GGE 2010	2010
	39UNGA Resolution 57/239: Creation of a global culture of cybersecurity	2003
Specialized agency conferences		
	40ITU, World Telecommunication Development Conference (Dubai, 2014) Resolution 45 – Mechanisms for Enhancing Cooperation on Cybersecurity, Including Countering and Combating Spam	2014
	41 ITU, Global Cybersecurity Agenda	2007
	42ITU, World Summit on the Information Society, Tunis Commitments	2005
Standards organizations		
	43US NIST, Framework for Improving Critical Infrastructure Cybersecurity 1.1	2017

	44 US NIST-NICE Cybersecurity Workforce Framework	2017
	45 US NIST, Guide to Cyber Threat Information Sharing	2016
	46 ISO 27001 -Information technology security techniques information security management systems – requirements	2013
	47 ISO 29147, Vulnerability disclosure to vendors	2014
	48 ISO 27032, Guidelines for Cybersecurity	2012
	49 ITU-T, X.1500 Cybersecurity information exchange – Overview of cybersecurity	2011
OSCE (Note: the OSCE is a region organization, categorized separately because of its engagement with CBMs.)		
	50 OSCE, Minsk Declaration	2017
	51 OSCE, Ministerial Council Decision 5/16, Efforts Related to Reducing The Risks of Conflict Stemming from the Use of ICTs	2016
	52 OSCE, Decision No. 1202 on Confidence-Building Measures to Reduce the R Conflict Stemming from the Use of ICTs	2016
	53 OSCE, Permanent Council Decision No. 1106	2013
INTERGOVERNMENTAL DECLARATIONS		
	54 BRICS, Leaders Xiamen Declaration	2017
	55 G20, Statement on Countering Terrorism	2017
	56 G7, Declaration on Responsible States Behavior in Cyberspace	2017
	57 G7, Principles and Actions on Cyber	2016
	58 BRICS, ICT Development Agenda and Action Plan	2016
	59 G20, Antalya Summit Leaders Communique	2015
	60 G7, Foreign Ministers' Meeting Communiqué	2015
NON-GOVERNMENTAL		

ORGANIZATIONS AND ACADEMIC INSTITUTIONS		
	61Carnegie Endowment, Toward A Global Norm Against Manipulating the Integrity of Financial Data	2017
	62CCDCOE, Tallinn Manual 2.0	2017
	63 Oxford Global Cyber Security Capacity Centre, Cybersecurity Capacity Maturity Model for Nations	2017
	64Carnegie Endowment (Europe), Governing Cyberspace: A Road Map for Transatlantic Cyberpolicy Leadership (pp. 74-75)	2016
	65Freedom Online Coalition, Tallinn Agenda for Freedom Online	2014
	66Netmundial, Multistakeholder Statement	2014
	67Stanford University, Draft International Convention to Enhance Protection from Cyber Crime and Terrorism	2001
INDUSTRY AND SECTORAL ORGANIZATIONS		
	68Facebook, Building Global Community	2017
	70Google, Digital Security & Due Process: Modernizing Cross-Border Government Access Standards for the Cloud Era	2017
	71Global Internet Forum to Counter Terrorism	2017
	72Microsoft/RAND, International Cyberattack Attribution Organization	2017
	73Microsoft, Digital Geneva Convention	2017
	74 ICANN, Draft Framework for Registry Operator to Respond to Security Threats	2017
	75Microsoft, From Articulation to Implementation: Enabling progress on cybersecurity norms	2016
	76Board of the International Organization of Securities Commissions, Guidance on cyber resilience for financial market infrastructures	2016
	77US Securities and Exchange Commission, Cybersecurity Guidance	2015
	78 ICANN, Montevideo Statement on the Future of Internet Cooperation	2013

LAW ENFORCEMENT AGENCIES		
	79Interpol, Global Cybercrime Strategy	2017
	80Europol, European Cybercrime Center (EC3), Joint Cybercrime Action Taskforce	2014
OTHER		
	81Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies	2017
	81.5 Meridian Process for Critical Information Infrastructure Protection	2005
	82Computer Emergency Response Team (CERT / CSIRT)	No date
	83 Information Sharing Analysis Centers	No date
	84 PCH, INOC-DBA	2002

SECTION 4: SELECTED OUTCOMES OF THE GAP ANALYSIS OF THE MATRIX WITH RESPECT TO THE MEASURES INCORPORATED INTO INITIATIVES

Some of the key outcomes are as follows:[105]

MEASURES THAT WERE INCORPORATED IN INITIATIVES

More than a quarter of the initiatives across the stakeholder categories (21/84) incorporated the following measures:

KEY #	OPERATIVE MEASURE	NUMBER OF INITIATIVES INCOR-PORATING THE MEASURE (OUT OF 84 TOTAL)
4.1	Information sharing measures in general (information about strategies, policies, legislation, best practices, capacity building)	43

[105] This summary of outcomes is intended to address the concern of one of the reviewers regarding the quantity of data in the graphic representation of the gap analysis. While the summary highlights key outcomes, others are inherent in the chart provided in Appendix 1. The methodological issue of the frequency parameter is addressed in Part II above.

19	Mechanisms for international cooperation (conferences, task forces, cyber diplomacy, learning exchanges, dedicated websites)	35
9	Mechanisms for government - private sector cooperation	31
5.3	Specific mechanisms for transnational law enforcement cooperation and mutual legal assistance for cybercrime	30
4.2	Establishment of a specific national or organizational point of contact for information exchange (including mandate or suggestion of CERT, CSIRT specifically)	29
6	Technical standards recommended or required	27
15	Creating a culture of cybersecurity or information security	25
4.6	"Regular dialogue"	23
4.3	Threat sharing (in general)	23
10	Mechanisms for government - third sector cooperation (NGO's, academia, civil society, informal groups)	22
3	Developing common terminology	21
8.2	Mechanisms for protecting critical infrastructure and essential services	19
4.4	Real-time, 24/7 exchange	18
18	Closing the digital divide	15
14	Cyber education programs	14
12	Supply chain supervision	13
5.1	General cybersecurity legislative measures are mandated	12
2	Publication of a cybersecurity strategy, policy and/or incident response plan required or recommended	11
20	Research and development (R&D) mechanisms mandated	11
4.5	Mechanisms should be established for communicating vulnerability disclosures	10
23	Publication of statistics, metrics and indicators mandated or recommended	10
11	Mechanisms for B2B cooperation	9
13	Development, training and certification of cybersecurity personnel	9
17	Conducting cyber simulation exercises and tabletops	9
8.1	Common CI (critical infrastructure) terminology	8
22	Development of risk assessment mechanisms for increasing cybersecurity, including insurance risk assessment	7
24	Ensuring technical interoperability of networks	7

7	Certification of professionals, products or services recommended or required	7
1	Specification of government institutions or entities responsible for cyber governance	6
4.7	Information Sharing and Analysis Centers (ISACs) mandated or suggested	6
21	Security / privacy by design for products, systems and services is recommended	6
5.5	Programs to educate and train national legislators and other legal/regulatory personnel on cybersecurity	6
27	Promotion of gender, youth and other diversity cyberspace workforce / engagement	5
5.2	Common definitions of cybercrimes	5
26	Promotion of e-governance	3
4.9	Cyber hotline for issues that may escalate	5
5.4	Mechanism for attribution of hostile cyber activities	2
16	Developing cybersecurity leadership	2
25	Utilize generic identity certificates (digital certification) for user authentication	2
4.8	FIRSTs mandated or suggested	1

SOME ADDITIONAL GAPS IDENTIFIED FROM THE ANALYSIS

Several additional gaps stem from the analysis of initiatives carried out in this Brief. These are listed below, and may serve as a basis for the development of policy recommendations in future iterations of the research on which the Brief is based.

- It is relatively acceptable to actors to agree to general arrangements for **information sharing** (#4.1 – 43 initiatives – it is the leading agreed-upon measure), and even to specify a national or organizational point of contact (#4.2 – 29 initiatives) but they are less willing to commit to a 24/7, real-time exchange of cybersecurity-related information (#4.4 – 18 initiatives).
- There appears to be a high degree of readiness to cooperate around **mutual legal aid and support in coping with cybercrime** (#5.3 - 30 initiatives). Yet support for such cooperation by collaborating on common definitions of cybercrimes (#5.2 – 5 initiatives) and by training legislators and judges (#5.5 – 6 initiatives) is less common.
- **Attribution** is a key issue for many aspects of cybersecurity and law enforcement regarding cybercrimes. Only Microsoft has been willing to propose a mechanism for advancing technical means attribution (#5.4 – 2 initiatives). The novelty of the proposal, as well as its challenge to the *status quo* of non-transparency for many activities in cyberspace, are probably strong contributing factors.
- Arrangements for **government cooperation with the private sector** (#9 –31 initiatives) **and civil society** (#10 – 22 initiatives) are relatively highly prioritized. Yet such arrangements are often plagued by lack of trust and efficiency.[106] This is an "external" gap (i.e., it is not evident from the analytical matrix), and it is somewhat surprising that 7 out of 10 private sector actors include this element in their initiatives.

[106] See, for instance, Andrew Nolan, *Cybersecurity and Information Sharing: Legal Challenges and Solutions*, Congressional Research Service, March 16, 2015.

- Finally, there are two measures that appear, *prima facie*, to be **relatively low cost/high gain modes of bolstering cybersecurity**, yet are not readily included in initiatives: research and development programs (#20 –11 initiatives) and instituting recommendations regarding security and privacy by design (#21 – 6 initiatives). The reasons for their non-inclusion are unclear, and are important to pursue through further research in terms of their feasibility and potential impact on cybersecurity.

CONCLUSION – TOWARDS A BASELINE OF MEASURES FOR STABILITY IN CYBERSPACE - NEXT STEPS

This Brief has focused on the analytical gaps identified with respect to the incorporation of measures into current cyber diplomatic initiatives; and the opportunities these gaps may present for bolstering global cybersecurity. Some of the key gaps have been identified above, and some of the opportunities that might be leveraged by future cyber diplomatic initiatives are discussed below.

STATE AND NON-STATE ACTORS ARE CLEARLY MOVING AHEAD WITH DIPLOMATIC INITIATIVES FOR INCREASING THE STABILITY OF CYBERSPACE.

Returning to the support referred to at the outset that was expressed by the 2015 GGE Report for "voluntary, non-binding norms of responsible State behavior", including CBMs and other measures: in the intervening two years state and non-state actors alike have moved ahead in precisely this direction. We have noted above that of the 84 initiatives identified and analyzed in this Brief, 83% date from 2012 to the present, and 53 of them – 63% - date from 2015 on. This is a remarkable indication of the current interest in moving forward with the normative and practical challenges of cyberspace.

A recent example of this continued interest and commitment, which contains many of the measures reviewed in this Brief, is the April 2017 G7 Declaration on Responsible States Behavior in Cyberspace. The G7 Declaration interweaves both norms and operative measures in a document that clearly presents the intent of its signatories, countries that are relatively advanced in their utilization of cyberspace and representing some of the world's strongest economies: [107] The approach of this recent cyber diplomatic initiative is worth noting:

> *We are committed to promoting a strategic framework for conflict prevention, cooperation and stability in cyberspace, consisting of the recognition of the applicability of existing international law to State behavior in cyberspace, the promotion of voluntary, non-binding norms of responsible State behavior during peacetime, and the development and the implementation of practical cyber confidence building measures (CBMs) between States....* [108]

Future diplomatic initiatives at the global, regional and domestic levels should to be able to build on this and similar flexible approaches.[109]

---

[107] The member countries are Canada, France, Germany, Italy, Japan, the United Kingdom and the United States.

[108] At p. 2 of the Declaration.

[109] On the importance of flexibility of approach and the importance of the process of norm-building, see also Finnemore and Hollis, note 2.

TWO POINTS OF CAUTION

Nevertheless, we offer two points of caution regarding the diplomatic initiatives reviewed in this Brief. First, like-minded countries that negotiate these initiatives may be in fact echoing one another, yet excluding many others: an unreasonable proposition in such a globally-connected context as cyberspace. One example of this is the potential redundancy, reiteration and cross-referencing in the initiatives analyzed here to the 2015 GGE Report, as opposed to a potential cumulative normative effect through incorporation in more separate initiatives. Initiatives of the G7, G20, and OAS refer to the Report; yet Russia, China[110] and the BRICS countries as a group, significant players in cyberspace, do not. Some of the normative dissonance does penetrate the mutual language barriers, yet there is an urgent need to learn firsthand about the cybersecurity needs of those countries that have agreements, protocols, policies, rules, guidelines and CBMs in languages or formats that are not currently accessible. This constraint is also an acknowledged methodological shortcoming of the present Brief.

Secondly, the metrics relevant to measuring the impact and success of cybersecurity norms and measures, even when consistently implemented by actors, are still evolving.[111] It is critical for cybersecurity initiatives and the policy processes that accompany them to incorporate more transparent data regarding the relevant cost-benefit analyses, to include the public more effectively in the discussion around these costs and benefits, and to elucidate parameters and proxies for impact and success of measures.

NEXT STEPS

Some of the initial findings of this Brief's gap analysis include a "convergence of concept" around several measures and CBMs to which different types of stakeholders have shown themselves willing to incorporate into initiatives. These measures are detailed in the analytical matrix and the accompanying analysis in Parts III and IV. To the extent that they provide a baseline from which diverse stakeholders might proceed to develop new potential zones of agreement, it is proposed that a good starting point would be those measures that have been identified in this Brief as the most frequently adopted by diplomatic initiatives. Additional analysis is required to elucidate whether the frequency of incorporation of these measures is due to their independent adoption in a variety of initiatives, or to redundancy in initiatives among similar stakeholders. Nonetheless, we propose in this Brief that this convergence of concept does indicate progress in the elucidation of the potential zones of agreement around measures for bolstering cybersecurity and at the international level.

These gaps identified remain very broad and generalized at this early stage of the research, making it a challenge to formulate a sense of the next steps needed for the formation of policy. Certainly, additional metrics need to be developed for better understanding the relationships among the diplomatic initiatives studied, as well as their potential impact.

Thus, the next stage of mapping, comparison and analysis for the development of global and national public policy with respect to IPS of cyberspace should address questions such as (a) the comparison of new initiatives to more mature ones; and (b) overlap or redundancy in stakeholders' incorporation of measures vs. cumulative and complementary take-up. Finally, to the end of influencing and leveraging future cyber diplomatic initiatives, a model for identifying proxies for impact and success of measures would deepen the understanding of which measures should be prioritized in public policy efforts.

---

[110] Except for the 2015 agreement with the US, which clearly referenced that year's GGE Report.

[111] See, for example, the evaluations and metrics used in Melissa Hathaway et al, *Cyber Readiness Index 2.0*, Potomac Institute, 2015.

SELECTED BIBLIOGRAPHY

Anna-Maria Osula and Henry Rõigas (Eds.), International Cyber Norms Legal, Policy & Industry Perspectives, CCDCOE, 2016.

Camino Kavanaugh, Tim Maurer, Eneken Tikk-Ringas, Baseline Review: ICT-Related Processes and Events, Implications for International and Regional Security, ICT4Peace Foundation, 2014.

James Lewis, Sustaining Progress in International Negotiations on Cybersecurity, Center for Strategic and International Studies, July 2017.

Martha Finnemore and Duncan B. Hollis, Constructing Norms for Global Cybersecurity, American Journal of International Law, Vol. 110, No. 3 (July 2016), pp. 425- 479.

Melissa Hathaway, Getting Beyond Norms: When Violating the Agreement Becomes Customary Practice, Centre for International Governance Innovation, 2017.

Paul Nicholas, What are confidence building measures (CBMs) and how can they improve cybersecurity?, Microsoft, 2017.

Vladimir Radunovic, Towards a secure cyberspace via regional cooperation, DiploFoundation, 2017.

APPENDIX 1

ANALYTICAL MATRIX REPRESENTING MEASURES IN CYBER DIPLOMATIC INITIATIVES ACCORDING TO TYPE OF STAKEHOLDER

*Please note that the number key for identifying initiatives appears in Figure 1.

ANALYTICAL MATRIX COMPARING CYBER INITIATIVES: OPERATIVE MEASURES														
INITIATIVES (KEY TO #'s BELOW) A. OPERATIVE MEASURES ▼		STATE-TO-STATE			UNI-LAT-ERAL STATE ON INTN'L PLANE	INTERNATIONAL ORGANIZATIONS				INTER-GOVERN-MENTAL DECLAR-ATIONS	NON-GOVERNMENTAL ORGANIZATIONS	INDUSTRY AND PRIVATE SECTOR	LAW ENFORCEMENT AGENCIES	OTHER
Tools and mechanisms, including CBM's, agreed upon or proposed by state or non-state actors to address IPS of cyber-space ("the how")		MULTILATERAL	REGIONAL	BILATERAL		UN	SPECIALIZED AGENCIES	STANDARDS	OTHER					
1	Specification of government institutions or entities respon-sible for cyber governance	2	7,13, 14,21, 22											

2	Publication of a cybersecurity strategy, policy and/or incident response plan required or recommended		13,21, 24,26				40,41	46		58	63	76,77		
3	Developing common terminology	2,3, 4,5	7,8, 13,14, 15,19, 21,23			38		45,48 49	52,53				79	81,82
4	Information sharing measures													
4.1	In general (strategies, policies Information about legislation, best practices, capacity building)	1,2, 4	6,7, 8,9, 11,13 14,16, 17,18, 20,21, 22,24, 25	27,28, 29,30	32,33, 34	35,37, 38,39	40	43,45 46,47 48,49	50,52 53	58	63,64, 66	71,76	79	81,82 83,84
4.2	Establishment of a specific national or organizational point of contact for information exchange (including mandate or suggestion of CERT, CSIRT specifically)	4	6,7, 9,13, 14,18, 19,20, 21,22, 23,25 ,	30,31	33,34	35,37		45,47 49	52,53	57		70,74		82,83

4.3	Threat sharing (in general)	4	6,7,9, 13,16, 20	27,28, 30,31		35		45,47 49	52	56,57	75	71	79,80	82,83
4.4	Real-time, 24/7 exchange	4	7, 13, 17,20, 23,25,	28,31	33	35		45,49					79,80	82,83, 84
4.5	Mechanisms shoul be established for communicating vulnerability disclosures		20			35		45,49	52	56	63	73,75, 76		
4.6	"Regular dialogue"	4	6,7, 9,11, 13,16, 17,18	27,28 30,31	32	35,37		45			66	71	79	81,82, 83
4.7	ISACs mandated or suggested		7					43,45				76,77		83
4.8	FIRSTs mandated or suggested											75		
4.9	Cyber hotline for issues that may escalate	2.5		30,31					52					84
5	Legislation, mutual legal assistance and													

	legal training													
5.1	General cybersecurity legislative measures are mandated	4	6,21, 22,23, 24,25	27			40		52		63		79	
5.2	Common definitions of cybercrimes	3,4	21,23								67			
5.3	Specific mechanisms for transnational law enforcement cooperation and mutual legal assistance for cybercrime	3,4	9,17, 19,21, 23,25	27,30	32,33, 34	35,37	40		52	56,57, 58, 60,61	63,67	70,74, 75	79	82,83
5.4	Mechanism for attribution of hostile cyber activities											72,75		
5.5	Programs to educate and train national legislators and other legal/regulatory personnel on cybersecurity		24	27	34						63	70	79	
6	Technical standards recommended or	2,5	6,7, 8,9, 11,13,	27	33,34		41	44,45 49		58	63,66	76		81,82 83

	required		14,20, 22,25, 26											
7	Certification of professionals, products or services recommended or required		7,8, 9, 14	27				44,49						
8	Critical infrastructure and essential services													
8.1	Common CI terminology	2,4	21					43			63,67			82,83
8.2	Mechanisms for protecting critical infrastructure and essential services	7	6,13, 22	27		35,37		43	52	56,58	63,67	72,73, 74,75, 76		82,83
9	Mechanisms for government - private sector cooperation	5	13,16 18,19, 21,22, 24,25, 26	27	33,34		42	43,45 47	52	55,56, 57,60	66	71,72, 73,74, 75,76, 78		82,83
10	Mechanisms for government - third sector cooperation (NGO's, academia, civil society, informal groups)	5	6,15, 16,18, 21,22, 24,26	27	34	35,37	42		52	56,57	66	71,72, 78		82,83

11	Mechanisms for B2B cooperation			27						58		71,72, 73,76, 78		82,83
12	Supply chain supervision		7	27	34			43,46 47		58	63	75,76, 77	79	81
13	Development, training and certification of cybersecurity personnel		6,7	27		35		45,46 48			63	76		
14	Cyber education programs		7,9, 13,15, 18, 21,22, 24,26	27		35,37			58		63			
15	Creating a culture of cybersecurity or information security	1	6,7, 9, 15, 18, 21,22, 24			35,38, 39	40,41, 42	43,45 46,48			63,66	73,76		82,83
16	Developing cybersecurity leadership		21					46						
17	Conducting cyber simulation exercises and tabletops		7,16 18,22	27		35,37						76,77		
18	Closing the digital divide	1,2, 5	18,22, 24		32,33	35,37	40,42			57,59	66			
19	Mechanisms for	2,4	6,7,	27,30,	32,33,	35,37			52,53	56,58	63,66		79	81,82

	international cooperation (conferences, task forces, cyber diplomacy, learning exchanges, dedicated websites)		9, 10, 11, 12,13, 14,15, 16,17, 18,19, 22,25	31	34									83
20	Research and development (R&D) mechanisms mandated		7,9, 13,17, 18,22	27		37				57,58		71		
21	Security / privacy by design for products, systems and services is recommended		13,14		33	39				57		76		
22	Development of risk assessment mechanisms for increasing cybersecurity, including insurance risk assessment		22					43	46,48		63	76,77		
23	Publication of statistics, metrics and indicators mandated or recommended		7,22,25 26				41	43				76	79	81,82
24	Ensuring technical			27	34			45,49			65,66	78		

	interoperability of networks													
25	Utilize generic identity certificates (digital certification) for user authentication						41,42							
26	Promotion of e-governance									58	63,65			
27	Promotion of gender, youth and other diversity cyberspace workforce / engagement	26		27						58	65,66			

ANALYTICAL MATRIX REPRESENTING NORMS IN CYBER DIPLOMATIC INITIATIVES ACCORDING TO TYPE OF STAKEHOLDER

The norms most frequently incorporated, in descending order, are as follows:

*Please note that the number key for identifying matrix initiatives appears in Figure 1 above.

	RANKING OF NORMATIVE ELEMENTS IN THE INITIATIVES ANALYZED	
KEY #	NORM	NUMBER OF INITIATIVES INCOR-PORATING THE NORM (OUT OF 84 TOTAL)

28.11	Human rights, civil rights, and/or individual rights should be respected in cyberspace	30
32	Norms relating to internet/cyberspace governance in general	28
36.1	Protection of personal and private data	25
37	Norms specifying international cooperation	26
28.1	UN Charter applies in cyberspace	18
31	Norms relating to critical infrastructure protection	17
28.2	International law applies in cyberspace	16
28.12	Endorsement of 2015 UNGGE norms	15
30.1	Prohibition of the use of cyberspace by non-State actors for terrorist and other criminal purposes (see also 2.2)	15
35.1	Responsibility to ensure the integrity of the ICT supply chain	15
36.3	Intellectual property protections	13
28.4	Other "international norms", "universally recognized norms" or "standards" apply in cyberspace (rather than "international law")	9
28.7	The principle of state sovereignty applies in cyberspace	8
28.3	"International rule of law" applies in cyberspace"	5
30.3	Terrorist content should be criminalized / removable	5
30.4	Child pornography or abuse online should be criminalized / removable	5
28.8	Self-defense / collective self-defense against other countries' use of force in cyberspace is permissible	5
29.2	State must not allow their territories to be used for wrongful acts in cyberspace	4
33	Protection of CERTs and other cyber emergency responders	4
36.2	Financial data protections when separate from 36.1)	4
34	Norms governing responsibility to report ICT vulnerabilities	3
35.2	Prevention of the proliferation of malicious ICT tools and techniques	3
28.10	Countermeasures are permissible	3
29.1	"Internationally wrongful acts" using ICT are forbidden in cyberspace	3
29.3	ICT should not be used for purposes that harm international security	3
30.2	Information should be prohibited that is inciteful or inflames hatred on	3

	ethnic, racial or religious grounds	
28.9	Cyberattacks against critical infrastructure are be equivalent to aggression	1
28.5	The promotion of voluntary norms of responsible state behavior in cyberspace	1
28.7	Appropriate norms of state behavior in cyberspace within the international community need to be identified and promoted	1
29.4	Private sector companies should not be targeted	1

FULL ANALYTICAL MATRIX FOR NORMS

ANALYTICAL MATRIX COMPARING CYBER INITIATIVES: NORMS

INITIATIVES ▶ (KEY TO #'s BELOW) / **B. NORMS ▼**		**STATE-TO-STATE**			**UNILAT-ERAL STATE ON INTN'L PLANE**	**INTERNATIONAL ORGANIZATIONS**				**INTERGOVERNMENTAL DECLARATIONS**	**NON-GOVERNMENTAL ORGANIZATI AND ACADEMIC INSTITUTIONS**	**INDUSTRY AND PRIVATE SECTOR**	**LAW ENFORCEMENT AGENCIES**	**OTHER**
Normative elements agreed upon or proposed by state or non-state actors to address IPS of cyber-space ("the what")		**MULTILATERAL**	**REGIONAL**	**BILATERAL**		**UN**	**SPECIALIZED AGENC**	**STANDARDS**	**OTHERS**					
28	**Applicability of in-ternational law norms to state and non-state actor activity in cyberspace**													
28.1	UN Charter applies in cyber-space	**1**	**12,16**	**27**	**32**	**35,37**	**42**		**51,52 53**	**55,56,57, 59,60**	**62**		**75**	
28.2	International law applies in cyberspace		**16,22**	**27**	**33**	**35,37**	**42**		**51,52 53**	**55,56,57, 59,60**	**62**			
28.3	"International rule of law" applies in cyberspace"				**32,34**		**42**			**55**			**70**	
28.4	Other "inter-national norms",	**1,2**	**12,16**		**32,33, 34**	**35**					**62**			

	"universally recognized norms" or "standards" apply in cyberspace (rather than "international law")									
28.5	The promotion of voluntary norms of responsible state behavior in cyberspace		**27**							
28.7	Appropriate norms of state behavior in cyberspace within the inter national community need to be identified and promoted		**30**							
28.7	The principle of state sovereignty applies in cyberspace		**12,23**	**29**	**32,33**	**35,37**			**62**	
28.8	Self-defense / collective self-defense against other countries' use of force in cyberspace is permissible		**16**		**34**			**56,57**	**62**	
28.9	Cyberattacks against critical infrastruc-ture are be equivalent to aggression						**50**			
28. 10	Countermeasures are permissible				**33**			**56**	**62**	
28. 11	Human rights, civil rights, and/or individual rights should be respected in cyberspace	**1,3, 4,**	**14,15 16,22**	**27**	**32,33, 34**	**35,36, 37** **40,42**	**51,52 53**	**55,56,57, 60**	**62,63, 65,66, 67**	**70,7**
28. 12	Endorsement of 2015 UNGGE norms *version unclear		**10, 12,17**	**27*, 30,31**	**33**	**35**	**51**	**56,57,59, 60**		**73,7**
29	Explicit prohibitions derived from applicability of international law norms to state and non-state actor activity in									

	cyberspace															
29.1	"Internationally wrongful acts" using ICT are forbidden in cyberspace	**2**			**32**							**62**				
29.2	State must not allow their territories to be used for wrongful acts in cyberspace					**35,37**				**56**		**62**				
29.3	ICT should not be used for purposes that harm international security	**1**			**32**	**35**										
29.4	Private sector companies should not be targeted													**73**		
30	Norms relating to cybercrime and cyberterrorism															
30.1	Prohibition of the use of cyberspace by non-State actors for terrorist and other criminal purposes (see also 2.2)	**1**	**21,23**		**32,34**	**36,37**	**42**			**55,56**		**62,67**		**71**	**79,80**	
30.2	Information should be prohibited that is inciteful or inflames hatred on ethnic, racial or religious grounds	**1,3**	**21**													
30.3	Terrorist content should be criminalized / removable	**4**	**21,23**		**34**									**71**		
30.4	Child pornography and abuse online should be criminalized / removable		**23**							**55**		**63**		**74**	**80**	
31	Norms relating to critical infrastructure protection	**1**	**6,13, 21**	**27**		**35**		**43**	**50,52**	**56**		**62,67**		**73,7 76**		**82,8**
32	Norms relating to internet/ cyberspace governance in	**1,2**	**15**	**27**	**32,33, 34**	**35,37**			**52,53**	**54,55,56, 57**		**64,65, 67**		**68,7 73,7 75,7**	**70,79**	**82,8**

	general												
33	Protection of CERTs and other cyber emergency responders			**27**		**35**		**56**		**75**			
34	Norms governing responsibility to report ICT vul-nerabilities		**20**				**47**			**73**			
35	Protection of the ICT supply chain												
35.1	Responsibility to ensure the integrity of the ICT supply chain	**1**	**6,9**	**27**	**33,34**	**35,37**	**43,**	**56**		**75,7 77**		**81**	
35.2	Prevention of the proliferation of malicious ICT tools and techniques					**35**				**73**		**81**	
36	Norms governing the protection of types of data												
36.1	Protection of personal and private data		**8,13, 14,19 21,22**		**32,33, 34**	**39**	**43, 46,**	**56,57,59, 60**	**63,64, 66,67**	**70,7 74**			
36.2	Financial data protections (when separate from 36.1)		**14**					**61**		**76,7**			
36.3	Intellectual property protections	**4**	**20**	**27,30**	**32,33, 34**		**45,**	**56,57,59**	**63**				
37	Norms specifying international cooperation												
		1,2, 4,5	**9,10, 15,20 22,25**	**27**	**32,33, 34**	**35,37**		**55,56**	**62**	**73,7 75**	**70,79**	**82,8**	