Promoting International Cyber Norms: A New Advocacy Forum

A Report from the EastWest Institute Breakthrough Group on **Promoting Measures of Restraint in Cyber Armaments**

December 2015

Promoting International Cyber Norms: A New Advocacy Forum

A Report from the EastWest Institute Breakthrough Group on
Promoting Measures of Restraint in Cyber Armaments

Principal Authors

Greg Austin, Professorial Fellow, EastWest Institute
Bruce McConnell, Global Vice President, EastWest Institute
Jan Neutze, Director of Cybersecurity Policy, Europe, Middle East and Africa (EMEA), Microsoft

Contributors

Shen Yi, Associate Professor and Executive Director, Workshop on the Studies of
National Cyber Security Strategy and Technology, Fudan University
John Savage, Professorial Fellow, EastWest Institute; An Wang Professor of Computer Science, Brown University

–

Illustrations by Dragan Stojanovski

The views expressed in this publication do not necessarily reflect the position of the EastWest Institute, its Board of Directors or staff.

–

The EastWest Institute works to reduce international conflict, addressing seemingly intractable problems that threaten world security and stability. We forge new connections and build trust among global leaders and influencers, help create practical new ideas, and take action through our network of global decision-makers. Independent and nonprofit since our founding in 1980, we have offices in New York, Brussels, Moscow and Washington.

–

The EastWest Institute
11 East 26th Street, 20th Floor
New York, NY 10010 U.S.A.
+1-212-824-4100

–

communications@eastwest.ngo
www.eastwest.ngo

Summary

Global security and prosperity depend on a secure and stable cyberspace. Events in 2015, especially agreement among the UN Group of Governmental Experts (GGE), hold out a new opportunity to lift the tempo of global advocacy of norms of state behavior in cyberspace. This opportunity has been framed by more than a decade of diverse and often uncoordinated activism by states, businesses and civil society. The stakeholders have not arrived at consensus on some of the most serious issues affecting international security, but we have reached a new plateau that allows us to usefully take stock and build on success. One key lesson we can draw is that the classic institutions of international organization, either governmental or in the business sector—the current regime complex—benefited from the availability of activist NGOs to achieve this new plateau. One reason for the successful role of NGOs was their ability to mediate perceptions of opposing sides.

The report recommends the establishment of a forum to help deepen consensus around emerging cyber norms and bridging remaining substantial divides on normative issues. This forum would have as its main goal the early take-up by states of norms of mutual restraint or norms of common welfare in cyberspace. The forum would begin by pursuing progress among states and other stakeholders on some specific norms, such as avoiding attacks on critical infrastructure, helping to build confidence that would support progress on broader norms related to military uses of cyberspace.

The need for the new forum arises from the opportunity described above. The value of such a forum rests on the ability of NGOs to get out in front of governments with new thinking. Yet, the need and value of a new standing forum are also driven by several dangerous considerations that have not been eliminated by the new plateau of consensus. These considerations, which demand greater action and focus by the NGO sector working with stakeholders (states, businesses and civil society), include:

- Continuing militarization of cyberspace by states, regardless of political system.
- Continuing securitization of cyberspace by states within their own borders, regardless of political system.
- Growing activism by multinational corporations and civil society around norm advocacy that does not fit neatly into the current gradualist approaches by states, not least because some corporations no longer see their government of national registration as representing their interests.
- Sector-based risks, for example in financial services and civil nuclear information security, that have not been adequately addressed in inter-state forums.
- Persistent asymmetries of power and knowledge among stakeholders, especially states, that fuels reluctance by them to commit early to new normative behavior.

Some states may oppose the creation of any new forum of the sort advocated by this paper. We heard an argument that it is states that dominate the space where international legal norms are decided, that progress has been remarkable, and that the current level of agreement among states contributes to escalation control should any security crisis emerge. Moreover, states are the only actors who can agree to new international legal norms, which can if necessary, be agreed upon quite quickly. There is also the consideration that some states have little political appetite for a new forum addressing norm development. It was argued that a disaggregated, sector-based approach might be more fruitful.

However, it has taken states ten years since the convening of the first GGE to agree on possible voluntary norms; and in the first significant opportunity presented at head-of-state level to take that up (a U.S./China summit in September 2015), the two leaders were able only to “welcome” the GGE report, not to commit to any of the voluntary norms therein, including specifically a mutual ban on cyber attacks on critical infrastructure.

This paper begins with a history of cyber norms development and why it has proceeded so slowly. It then outlines the functions of a new norms advocacy forum and the characteristics necessary to make it successful. The paper concludes with an analysis of emerging consensus norms across five key global organizations, followed by lessons learned from the historical experiences of the EastWest Institute.

Comments may be sent to cyber@eastwest.ngo.

Progress on Norms of State Behavior in Cyberspace

Governments have long recognized the need to partner with business and civil society in framing new approaches to international norms and normative behavior in cyberspace. The process has been developing over almost a decade, but has been slow to gather momentum and consistency. The international community now has a unique opportunity to ramp up its efforts. The character of this opportunity is revealed more fully by the coincidence of the following events:

- UN Group of Governmental Experts (UNGGE) agreement in 2015 on several priority areas for normative behavior.
- A commitment to continued action by the government of the Netherlands after the fourth Global Conference on CyberSpace in The Hague in April 2015.
- General commitments in 2015 between Russia and China and China and the United States to normative behaviors toward each other in cyberspace.
- Progress on various multi-stakeholder processes, including NetMundial and the work of NGOs, especially by the EastWest Institute and ICT4Peace.
- Achievement of a critical mass in expert analysis of global approaches to norms and normative behavior through the work of organizations like the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn (Tallinn Manual on the International Law Applicable to Cyber Warfare) and corporations like Microsoft.
- Formation in 2014 of a Global Commission on Internet Governance.

The importance of new normative behaviors has been advocated in many places, along with principles and recommendations. For example, apart from many excellent academic works,[1] in 2013, Microsoft issued a useful paper outlining "Five Principles for Shaping Cyber Security Norms." The work of the UNGGE is itself testimony to recognition of the need, if not to its urgency.

- Work of the EastWest Institute, IEEE, CCDCOE in Tallinn, the Harvard Belfer Center, Center for Strategic and International Studies, China Institute of Contemporary International Relations, ICT4Peace, the UN Institute for Disarmament Research, (and many other researchers and organizations) mostly beginning in 2009 or later.
- The International Telecommunication Union's High Level Expert Group on Cyber Security in 2009.
- The World Federation of Scientists in 2008.
- The World Summit on Information Society between 2002 and 2005.
- The UN General Assembly in annual resolutions beginning in 1998.

Through these and other efforts, a variety of documents have emerged that propose norms of state behavior designed to mitigate or reduce certain malicious activity in cyberspace. Among these documents there is considerable convergence. We have chosen five reference documents for comparative analysis:

- Code of Conduct proposed by China, Russia and others, January 2015 (CoC).[2]
- U.S. Policy, from remarks by U.S. Secretary of State John Kerry in Seoul, May 2015 (USG).[3]
- United Nations Group of Governmental Experts on Information Security, August 2015 (UNGGE).[4]

[1] Michael Portnoy and Seymour Goodman (eds), *Global Initiatives to Secure Cyberspace: An Emerging Landscape*, New York: Springer, 2009; M. Maybaum, A.-M. Osula, L. Lindström (eds), *Architectures in Cyberspace*, Tallinn: CCDCOE, 2015; Nye, op. cit.; Michael N. Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge: Cambridge University Press, 2013; Michael N. Schmitt and Liis Vihul, "The Nature of International Law Cyber Norms," Tallinn Paper No. 5, Special Expanded Issue, Tallinn: CCDCOE, 2014; Roger Hurwitz, "The Play of States: Norms and Security in Cyberspace," *American Foreign Policy Interests*, vol. 36, no. 5, pp.322-331, 2014; Ludovica Glorioso and Anna Maria Osula (eds), *1st Workshop on Ethics of Cyber Conflict: Proceedings,* Tallinn: CCDCOE, 2014; "A Call to Cyber Norms: Discussions at the Harvard-MIT-University of Toronto Cyber Norms Workshops, 2011 and 2012," Belfer Center, Harvard University, 2015; Tim Maurer, "Cyber Norm Emergence at the United Nations," Belfer Center, Harvard University, 2011; Eneken Tikk-Ringas, "Developments in the Field of Information and Telecommunications in the Context of International Security: Work of UN First Committee 1998-2012," Geneva: ICT4Peace, 2012; Camino Kavanagh, Tim Maurer and Eneken Tikk-Ringas, "Baseline Review: ICT-Related Processes & Events: Implications for International and Regional Security (2011-2013)," Geneva: ICT4Peace, 2014; Abdul Paliwala, "Netizenship, security and freedom," *International Review of Law, Computers and Technology*, vol. 27, nos. 1-2, pp.104-123, 2013.

[2] "International Code of Conduct for Information Security," United Nations A/69/723, January 9, 2015, http://www.un.org/ga/search/view_doc.asp?symbol=A/69/723. The members of the Shanghai Cooperation Organization are: China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan and Uzbekistan.

[3] "An Open and Secure Internet: We Must Have Both," John Kerry, May 18, 2015, http://www.state.gov/secretary/remarks/2015/05/242553.htm.

[4] "Developments in the Field of Information and Telecommunications in the Context of International Security," United Nations A/70/174, July 22,

- NATO Tallinn Manual, 2013 (Tallinn).[5]
- Microsoft norms paper, *International Cybersecurity Norms: Reducing Conflict in an Internet-dependent World*, December 2014 (MSFT).[6]

These documents cover a broad variety of areas related to cyberspace policy. We have focused on the portions of each document that propose a norm of behavior directed at reducing certain malicious activity in cyberspace. It should be noted that since the UNGGE report represents an agreement among experts from the United States, Russia and China, among others, the UNGGE language could point towards a compromise between the proffered language in the CoC and USG sources referenced above.[7] These proposed norms fall into five general categories:

I. Basic principles ensuring the security and stability of global cyberspace.
II. The responsibility of states to avoid and to prevent certain types of cyber attacks launched from their territories.
III. The responsibility of states to enhance the security of information and systems within their territories.
IV. The duty of states to cooperate with each other to mitigate certain types of cyber incidents.
V. Restraint in the development or use of cyber weapons in peace time.

In each category, at least two of the reference documents propose one or more norms of state behavior. Appendix I lays out the text and briefly analyzes the areas of agreement and disagreement.

The Need to Move Faster

In spite of this unprecedented opportunity, there is no forum dedicated to advocating and speeding up norm development by states and other stakeholders by promoting international agreements, regimes of practice, habits of cooperation and confidence-building.

Figure 1 shows a representation of the existing "regime complex" governing cyberspace norm development, monitoring and observance developed by Joseph Nye.[8]

Joseph Nye concludes that we are unlikely to see a "single overarching regime for cyberspace any time soon."[9] He talks correctly of a "good deal of fragmentation" and says it "is likely to persist." He observes that "different sub-issues are likely to develop at different rates, with some progressing and some regressing in the dimensions of depth, breadth and compliance." Nye demonstrates this by identifying quite different areas of norm development for cyber activities (such as war, espionage, human rights, privacy, content control and standards) and the current regime state in these areas by depth, breadth, fabric and compliance.[10] He cites Keohane and Victor, who describe the field of climate change policy development as "actually many different cooperation problems, implying different tasks and structures."[11] They concluded that collaboration outcomes in each problem would sit variously on a scale of integration and fragmentation in large part because of divergences in "power weighted" interests, the potential for gains or losses from linking sub-issues, and differences in how actors managed uncertainty.

2015, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174. The participants in the 2014-2015 UNGGE for Information Security are: Belarus, Brazil, Canada, China, Colombia, Egypt, Estonia, France, Germany, Ghana, Israel, Japan, Kenya, Malaysia, Mexico, Pakistan, Russian Federation, Spain, United Kingdom and United States of America.

[5] "Tallinn Manual on the International Law Applicable to Cyber Warfare," NATO Cooperative Cyber Defence Centre of Excellence, 2013, https://ccdcoe.org/tallinn-manual.html. The Manual does not represent the views of NATO or its sponsoring nations. In particular, it is not meant to reflect the NATO doctrine.

[6] Paul Nicholas, "Proposed Cybersecurity Norms to Reduce Conflict in an Internet-dependent World," Microsoft, December 14, 2014, https://blogs.microsoft.com/cybertrust/2014/12/03/proposed-cybersecurity-norms/.

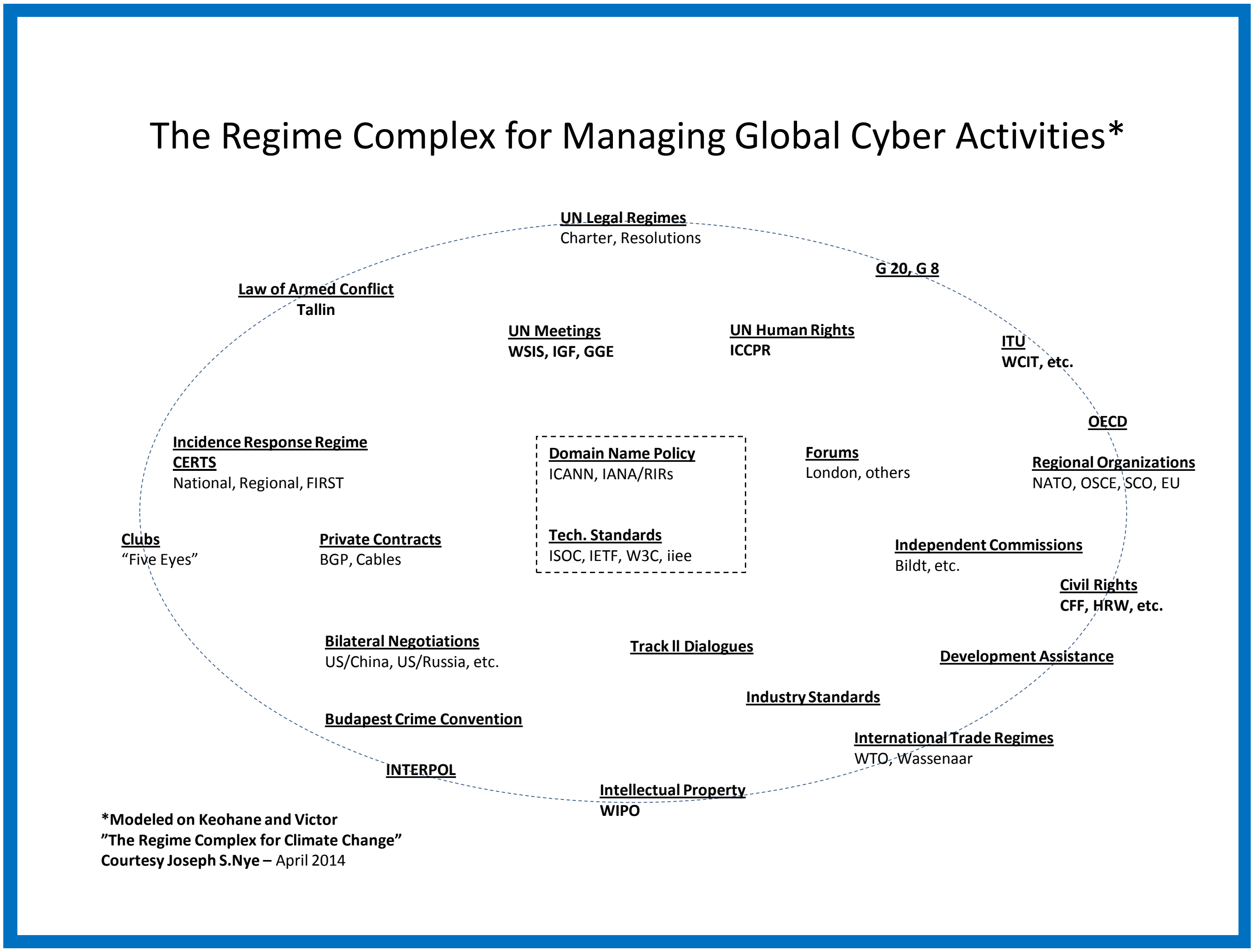
[7] We note the usefulness of the November 2015 G20 agreement. For more information, see: http://www.g20.utoronto.ca/2015/151116-communique.html.

[8] Joseph S. Nye Jr., "The Regime Complex for Managing Global Cyber Activities," Belfer Center, Harvard University, 2014, p.7, http://belfercenter.hks.harvard.edu/files/global-cyber-final-web.pdf.

[9] *Ibid*. p.15.

[10] *Ibid*. p.8.

[11] Robert O. Keohane and David G. Victor, "The Regime Complex for Climate Change*," Perspectives on Politics*, vol. 9, no. 1, p.8, 2011.



The Regime Complex for Managing Global Cyber Activities*

UN Legal Regimes
Charter, Resolutions

G 20, G 8

Law of Armed Conflict
Tallin

UN Meetings
WSIS, IGF, GGE

UN Human Rights
ICCPR

ITU
WCIT, etc.

OECD

Incidence Response Regime
CERTS
National, Regional, FIRST

Domain Name Policy
ICANN, IANA/RIRs

Forums
London, others

Regional Organizations
NATO, OSCE, SCO, EU

Clubs
"Five Eyes"

Private Contracts
BGP, Cables

Tech. Standards
ISOC, IETF, W3C, iiee

Independent Commissions
Bildt, etc.

Civil Rights
CFF, HRW, etc.

Bilateral Negotiations
US/China, US/Russia, etc.

Track II Dialogues

Development Assistance

Industry Standards

Budapest Crime Convention

International Trade Regimes
WTO, Wassenaar

INTERPOL

Intellectual Property
WIPO

***Modeled on Keohane and Victor**
"The Regime Complex for Climate Change"
Courtesy Joseph S.Nye – April 2014

Figure 1: Nye's Cyber Regime Complex

These perspectives are helpful in explaining the institutional reality and also in turning actors toward more clarity about the nature of the problem and problem-solving pathways. But they are rooted in a traditional framing of international relations that privileges not just hierarchy but also states.

A New Organization Could Help

For the very reasons that Nye identifies, and based on extended consultation by the EastWest Institute, this regime complex would benefit from an additional forum that can help reconcile the competing "weighted" interests and overcome the imbalances. This paper proposes such a new forum. Figure 2 shows a visual representation of where a proposed new forum might sit relative to key interest groups and the existing regime complex. The main target of action by this forum would still be states (as portrayed in the maroon arrow). One reason for this is that states are the actors most able to shape international security, including human security. (Security, broadly defined, remains the central concern of the EastWest Institute). Another reason is that the main gap in policy mobilization is not only among states, but between states and the other newly influential private stakeholders.

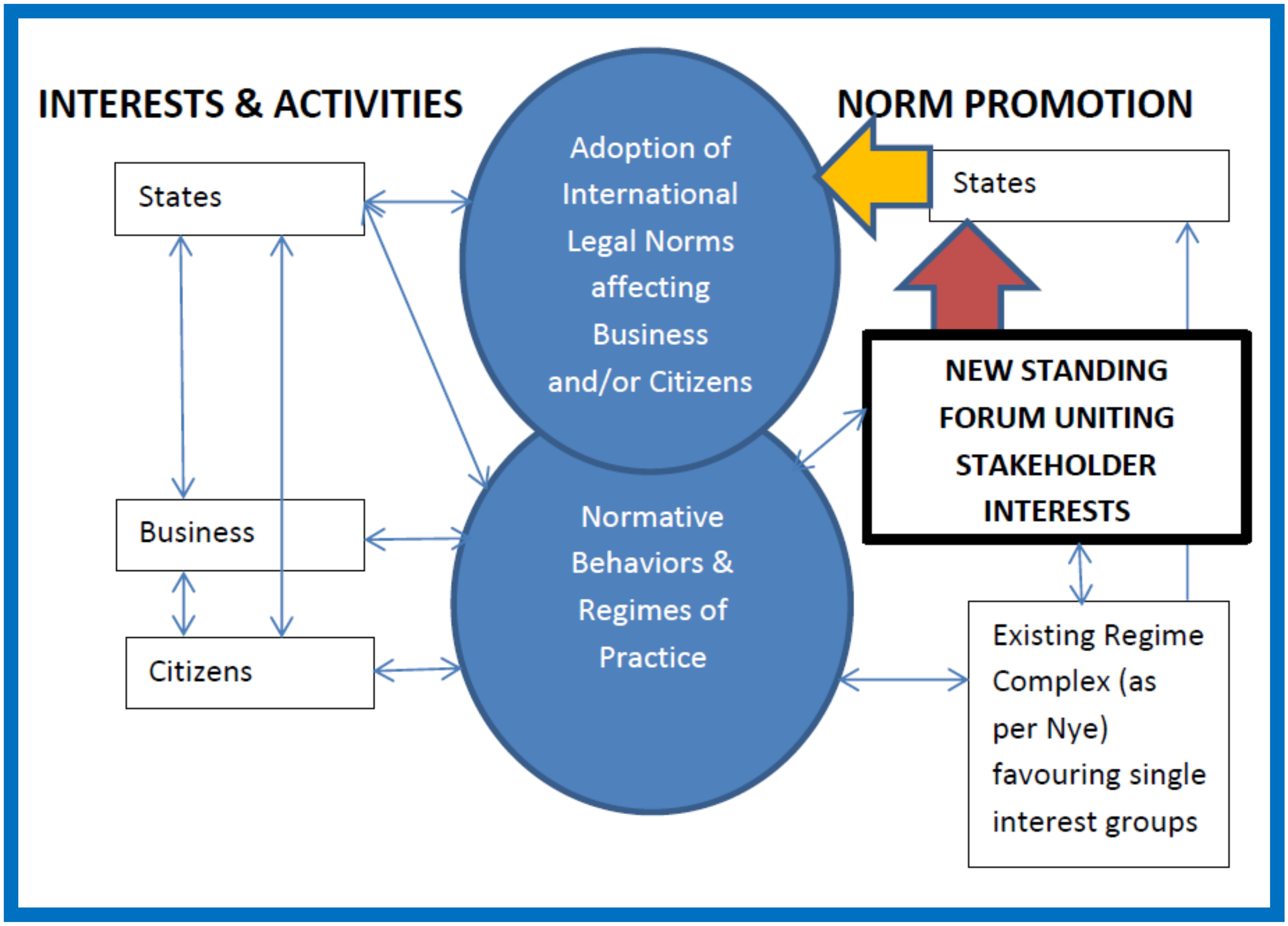

INTERESTS & ACTIVITIES
NORM PROMOTION
States
Adoption of International Legal Norms affecting Business and/or Citizens
States
NEW STANDING FORUM UNITING STAKEHOLDER INTERESTS
Business
Normative Behaviors & Regimes of Practice
Citizens
Existing Regime Complex (as per Nye) favouring single interest groups

Figure 2: Positioning of a New Forum

The strongest argument in favor of the proposed new forum may be the high degree of contestation about cyber norms relating to military uses of cyberspace, which most proposals do not address. Another strong argument, quite different, is that multinational corporations are moving to fill gaps left by states through direct participation in norm entrepreneurship. Yet another argument is that the fast pace of technological development in cyberspace creates such pressures that an NGO-led standing forum would provide a consistent and immediately available location for canvassing of proposed new norms. All worthy proposals should be discussed widely, but may not ultimately be regarded as practicable for formal dialogue among states. Such a new forum could also catalogue differences among states about behavior or actions by states regarded as unacceptable, without being partisan.

Since norms develop through socialization, any new forum would have to meet a test of how well it might contribute to that process. Advocates of a new forum believe that this may also be a particular strength, especially since it could help promote the overarching goal of strategic stability in cyberspace, which is still not agreed upon among major parties. There appears to be strong support internationally in having a standing "bridging mechanism," a clearing house of ideas and policy action that takes its position at an intermediate level—connecting states, business interests, professional expertise and civil society interests. This would play off the relationship between collaboration on technical issues and trust-building among all actors on higher level issues, including those exclusively in the preserve of states. For many, this seemed to be an inevitable conclusion from high levels of interest from all stakeholder groups shown in the EastWest Institute's work on norms in cyberspace cooperation beginning in 2009. This helped catalyze the London process in late 2011, and the emerging Netherlands proposal for some form of standing facility or organization, an idea that emerged from The Hague cyberspace conference in 2015. One might also draw a similar conclusion from the commitment of key stakeholder groups to the work of other NGOs and research centers in more specialized areas, such as ICT4Peace, the Information Security Institute at Moscow State University, its associated consortium, Harvard's Belfer Center, the Center for Strategic and International Studies in Washington, D.C. and the UN Institute for Disarmament Research.

On the other hand, EastWest's work in this area, including discussions at its sixth Global Cyberspace Cooperation Summit, elicited arguments against the kind of new standing forum being proposed. The effort put into existing forums at the intergovernmental level had been substantial and productive. The full potential of many existing forums, such as the possible role of the G20 in addressing cyber concerns specific to the financial services sector, may not have been fully exploited yet. Useful ideas raised by the EastWest Institute in respect to the civil nuclear sector[12] could be brought to the processes associated with the Nuclear Non-Proliferation Treaty (NPT) and the International Atomic Energy Agency (IAEA). Some argue that it is states that dominate the space where international legal norms are decided, that progress has been remarkable, and that the current level of agreement among states contributes to escalation control should any security crisis emerge.

Moreover, states are the only actors who can agree on new international legal norms, which can if necessary, be agreed upon quite quickly. One view held that states' consideration of a potential treaty for norms in cyberspace is still an important goal that states alone could address. Even if no treaty resulted, an interim step such as a code of conduct or voluntary norms might well be adequate. We also had to recognize that states' discussion to date of a possible treaty had, without producing that result, been very fruitful in promoting normative behavior and a measure of consensus.

There is also the consideration that some states have little political appetite for a new forum addressing norm development. In that light, it was argued that a disaggregated, sector-based approach relying on existing forums, might be more fruitful. The emerging role has been assigned by states to national Computer Emergency Response Teams (CERTs) in normative discussions, including in the UNGGE, and was seen by some as an important new locus of multilateral coordination on normative behavior that may obviate the need for the new forum.

Yet another view held that while there is indeed urgent need for discussion of military[13] aspects of cyberspace, it may be too early for any new NGO-led forum to discuss normative approaches—either for confidence building measures (CBMs) or treaty language—that depended on definitions of cyber weapons or indeed what constituted cyber armaments. Restraint in cyberspace may depend far more on "sincerity" of great powers in respect of the goal of strategic stability. If that does not exist, then CBMs or measures of restraint would be irrelevant.

NGO-led Norms Entrepreneurship Can Work

One of the best sets of guidance for NGOs involved in norm entrepreneurship has been framed by Dr. Morten Bergsmo, who was prominent in the establishment and work of the International Criminal Court (ICC). In 2004, two years after the ICC's formation, Bergsmo gave a detailed oral assessment of setting up the ICC at an NGO roundtable in Brussels.[14] Having noted how most international lawyers and politicians laughed at the idea of an ICC when it was first mooted, he identified the underlying normative foundations for the court, such as the Nuremberg principles. He also noted the advances in international criminal jurisdiction made during the 1990s, beginning with the UN Security Council decision to set up a Committee of Experts and followed by other measures, both within the International Law Commission and in practice (especially Security Council acquiescence in use of a Special Representative of the Secretary General in two different missions of war crimes authority). He noted the effect of the creation of other conflict specific tribunals in Yugoslavia, Sierra Leone and Cambodia on acceptance of the idea of an ICC.

Most importantly, for the purpose of significant reform in the international legal framework, Bergsmo identified six essential factors:

1. NGO mobilization and unity.
2. Competent, well-informed specialists and lawyers in those NGOs.
3. Sufficient transparency in the multilateral process for NGOs to be effective.
4. A few principled states to protect the integrity of the idea throughout the reform deliberations.

[12] Greg Austin, Eric Cappon, Nadiya Kostyuk and Bruce McConnell, "A Measure of Restraint in Cyberspace: Reducing Risk to Civilian Nuclear Assets," EastWest Institute, 2014, https://cybersummit.info/sites/cybersummit.info/files/A%20Measure%20of%20Restraint.pdf.

[13] We note that traditional strategic stability, i.e., controls on nuclear weapons, depends in part on command and control systems that may be vulnerable to cyber risks.

[14] These notes were provided by Greg Austin, organizer of the 2006 roundtable, on behalf of several prominent European think tanks and support by the Alliance of Liberals and Democrats in the European Parliament. The discussions were documented and reviewed contemporaneously by the participants.

5. Adequate great power acceptance to provide hard political legitimacy.
6. Established NGO "laboratories" to show the feasibility of the project.

Bergsmo noted the difference between "codification" as the concrete manifestation of existing state practice or norms of custom accepted as law, and "codification" designed to be a vehicle of reform or change with a view to "positivizing" a norm or ideal rather than a specific rule.

In the same roundtable, participants agreed that a similar set of ingredients had contributed to the success of the campaign to ban landmines, resulting in the Ottawa Treaty, and in the campaign for international regulation of the arms trade, especially small arms, which resulted over a slightly longer period in the UN Arms Trade Treaty.

Specific Characteristics of the Forum

Based in part on the considerations outlined above, we can propose that some of the forum's essential characteristics would be:

- A focus on early take-up by states of new norms of mutual restraint.
- An equal focus on early take-up by all stakeholders of new norms of common welfare in cyberspace.
- Particular attention to issues where there is large-scale intermingling among governmental, business and/or citizen interests.
- Geopolitical neutrality even while seeking to pressure states toward earlier agreement on new norms than might be possible if states were left to their own devices.[15]
- Enjoys the support of at least three well-placed states, three well-placed corporations and three well-placed civil society organizations as enduring partners and champions.
- Enjoys the broad and consistent support of other leading states (e.g. those in the UNGGE and their peers) and related international actors (ICANN and ITU), as well as their active participation in its work.
- Annual review and analytical function (stock-take) regarding stakeholder behavior in cyberspace and suggested norms.
- Commitment to more vigorous and effective programs of advocacy around the general goal of normative behavior, more than any other NGO has been able to deliver so far.
- Mobilizes critical analysis by scholars and stakeholders from around the world.
- Secures commitments to move faster and produce outcomes that help catalyze existing forums.
- Represents multi-stakeholder interests better than existing forums.
- Establishes early claims to be an entirely appropriate adjunct to state action and an effective adjunct to state action.
- Profiles new approaches, especially from states, businesses or citizens outside the dominant discourses of the West that have not yet gained traction or been treated appropriately in existing forums.
- Secures a nimble organizational structure but a permanent staff adequate to the task.
- Sustains funding of at least $2 million per year, preferably closer to $4 million.

Conclusion

As suggested earlier, the government of the Netherlands is considering the creation of an organization like that recommended here. The experience of the EastWest Institute in prioritizing international work across the broad array of cyberspace policy issues as part of its Global Cooperation in Cyberspace Initiative may be relevant here. At EWI, we aim to address the most intractable issues of international security where we can convene the right stakeholders, reframe the questions, create innovative solutions and mobilize for action.[16] We look forward to cooperating on the design and creation of any new organization that will take on this norms mission.

[15] This characteristic requires an understanding of the differing assumptions that may be in play across states. Appendix II provides a brief description of that landscape.

[16] Appendix III provides highlights of EastWest's work in this area.

Appendix I

I. Basic principles ensuring the security and stability of global cyberspace.

From CoC, two:

(1) To comply with the Charter of the United Nations and universally recognized norms governing international relations that enshrine, inter alia, respect for the sovereignty, territorial integrity and political independence of all States, respect for human rights and fundamental freedoms and respect for the diversity of history, culture and social systems of all countries.

(7) To recognize that the rights of an individual in the offline environment must also be protected in the online environment; to fully respect rights and freedoms in the information space, including the right and freedom to seek, receive, and impart information, taking into account that [international law][17] attaches to that right special duties and responsibilities....

From USG, one:

Acts of aggression are not permissible. And countries that are hurt by an attack have a right to respond in ways that are appropriate, proportional, and that minimize harm to innocent parties.

From UNGGE, two:

a. Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security.

e. States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression.

Analysis: The norms here recognize the kinds of balance that are often found in international agreements between the rights of states to defend themselves against internal and external threats and the need for action to maintain international peace and security. For example, the U.S. statement, "Acts of aggression are not permissible," is balanced by an assertion of the "right to respond." There are, of course, differing views on such language, whether the response is in cyberspace or through diplomatic or other means. Some would say it enhances peace and stability by creating a deterrent, while others would impute a destabilizing threat. Indeed, in a draft convention on cyberspace tabled by Russia in 2011, reference was made to "acts of aggression" as one of the main threats in cyberspace (Article 4.1) and reference was also made to the right of states to retaliate against such aggression (Article 5.11).[18] The 2011 version of the CoC also contained a specific reference to "acts of aggression." However, the 2015 version of the CoC dropped the reference and confined itself to "not to carry out activities which run counter to the task of maintaining international peace and security."

[17] The full text reads, ". . . the International Covenant on Civil and Political Rights (article 19) attaches to that right special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) for respect of the rights or reputations of others; (b) for the protection of national security or of public order (ordre public), or of public health or morals."

[18] Ministry of Foreign Affairs of the Russian Federation, *Convention on International Information Security (Concept)*, 2011, http://archive.mid.ru//bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/7b17ead7244e2064c3257925003bcbcc!OpenDocument.

II. The responsibility of states to avoid and to prevent certain types of cyber attacks launched from their territories.

From the CoC, two:

(2) Not to use information and communications technologies and information and communications networks to carry out activities, which run counter to the task of maintaining international peace and security.

(3) Not to use information and communications technologies and information and communications technologies networks to interfere in the internal affairs of other States or with the aim of undermining their political, economic and social stability.

From the USG, three:

No country should conduct or knowingly support online activity that intentionally damages or impedes the use of another country's critical infrastructure.

No country should conduct or support cyber-enabled theft of intellectual property, trade secrets, or other confidential business information for commercial gain.

Every country should mitigate malicious cyber activity emanating from its soil, and they should do so in a transparent, accountable and cooperative way.

From the UNGGE, two:

c. States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs.

f. A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public.

From Tallinn, one:

5. A State shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States.

Analysis: The USG, Tallinn, and UNGGE positions calling on states to "mitigate malicious cyber activity emanating from its soil," "not knowingly allow their territory to be used for internationally wrongful acts," and "not knowingly allow the cyber infrastructure located in its territory … to be used for acts that adversely and unlawfully affect other States" suggest that if a state becomes aware that some third party—whether an individual, group of individuals, another state, or, perhaps an apparatus of the state itself—is using the ICT infrastructure within its territory for internationally wrongful acts, that state has a responsibility to try to stop the activity. In the non-cyber world, states have long been able to arrest or extradite other individuals suspected of committing piracy, slavery or genocide. While the language in the CoC is narrower, Russian and Chinese experts' support of the language in the UNGGE report may signal an evolution of their formal positions. There appears to be wide agreement on this kind of norm. Work remains to clarify in practical terms the extent of state responsibility for prevention or mitigation of malicious cyber acts. Of special note, neither the UNGGE nor the CoC refer to commercial cyber espionage by states. It may also be noted that China and the U.S. have accepted that state-supported or conducted commercial cyber espionage for the benefit of domestic companies from their territories is contrary to its international agreements.

III. The responsibility of states to enhance the security of information and systems within their territories.

From the CoC, two:

(5) To endeavor to ensure the supply chain security of information and communications technology goods and services….

(6) To reaffirm the rights and responsibilities of all States, in accordance with the relevant norms and rules, regarding legal protection of their information space and critical information infrastructure against damage resulting from threats, interference, attack and sabotage.

From UNGGE, three:

g. States should take appropriate measures to protect their critical infrastructure from ICT threats….

i. States should take reasonable steps to ensure the integrity of the supply chain so end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions.

j. States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure.

From Tallinn, two:

1. A State may exercise control over cyber infrastructure and activities within its sovereign territory.

2. Without prejudice to applicable international obligations, a State may exercise its jurisdiction: (a) over persons engaged in cyber activities on its territory; (b) over cyber infrastructure located on its territory; and, (c) extraterritorially, in accordance with international law.

From MSFT, two:

1. States should not target ICT companies to insert vulnerabilities (backdoors) or take actions that would otherwise undermine public trust in [commercial] products and services.

2. States should have a clear principle-based policy for handling product and service vulnerabilities that reflects a strong mandate to report them to vendors rather than to stockpile, buy, sell, or exploit them.

Analysis: Secure infrastructure depends significantly on secure technology. Microsoft's first proposed norm, regarding the insertion by states of vulnerabilities in commercial ICT products and services companies, is unsurprisingly stronger than the government-led UNGGE recommendation that states take reasonable steps to maintain the integrity of the supply. Similarly, a key aspect missing from the government-centric UNGGE effort would be an additional norm limiting government action to undermine international security standards efforts to benefit their own interests.

This aspect of the norm will come under increasing scrutiny as the debate about "ubiquitous encryption," and law enforcement access to communications content under legal process moves into the global policy environment.[19] The Kerry speech (USG) does not address the responsibility for securing systems within national boundaries as an international norm, perhaps because it is seen as a domestic matter. However it is certainly true that the U.S. government is taking steps to secure U.S. critical infrastructure.[20] The same can be said of most of the UNGGE participating governments.

[19] For two different U.S. perspectives, see: Mike McConnell, Michael Chertoff and William Lynn "Why the fear over ubiquitous data encryption is overblown," *Washington Post*, July 28, 2015, https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html; and: Cyrus R. Vance, Jr., François Molins, Adrian Leppard and Javier Zaragoza, "When Phone Encryption Blocks Justice," *The New York Times*, August 11, 2015, http://www.nytimes.com/2015/08/12/opinion/apple-google-when-phone-encryption-blocks-justice.html?_r=0.

[20] See: *inter alia,* Executive Order No. 13636, "Improving Critical Infrastructure Cybersecurity;" Presidential Policy Directive (PPD)-21, "Critical

IV. The duty of states to cooperate with each other to mitigate certain types of cyber incidents.

From the CoC, one:

(4) To cooperate in combating criminal and terrorist activities that use information and communications technologies and information and communications networks, and in curbing the dissemination of information that incites terrorism, separatism or extremism or that inflames hatred on ethnic, racial or religious grounds.

From the USG, one:

Every country should do what it can to help states that are victimized by a cyberattack.

From the UNGGE, two:

b. In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences.

h. States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty.

From MSFT, one:

6. States should assist private sector efforts to detect, contain, respond to, and recover from events in cyberspace.

Analysis: Increasingly in cyber incidents, information on combating threats is not only, or even primarily, in the hands of a national government response team. In the hours and days after an incident, multiple actors—from other countries—often contribute to identifying and then solving the issue. Today, information sharing often begins as an ad hoc collaboration, particularly during a crisis that aligns disparate sectors and even competitors toward a unified, collective response. For example, in 2008, the Conficker Working Group came together to share information and develop a response to the Conficker worm which had infected millions of computers around the world. Similarly, in the recent attacks against Sony Entertainment, corporate and government teams from several countries worked together to mitigate the effects of the attacks. Participants in these responses were willing to share information because there was a mutual benefit to be gained from the collective response, not least the trust developed between the responders, notably between government responders and private sector participants.

The various norms proposed in this “mutual assistance” section have the potential to enhance and further drive existing models of collaboration. Effective incident response efforts depend both on the maturity of public and private sector response capabilities as well as trusted relationships to enable information-sharing between them. Norms can help foster trust and build confidence, but they are not in themselves sufficient. Ongoing operational, functional, pragmatic cooperation and enhanced transparency around policies and response structures are vital elements in this context.

Cooperation can become more challenging when “curbing the dissemination of information that incites terrorism, separatism or extremism or that inflames hatred on ethnic, racial or religious grounds” (SCO-4). Differing standards across cultures can make for disagreements at the margins about what content falls under free speech, however offensive it may be. Continued dialogue will increase understanding here, but differences will remain.[21]

Infrastructure Security and Resilience;” both are from February 12, 2013. More recently, see*,* “Cybersecurity Enhancement Act of 2014,” P.L. 113-274, December 18, 2014.

[21] The work of Internet & Jurisdiction Project (www.internetjurisdiction.net) is instructive and useful in this regard.

V. Restraint in the development and use of cyber weapons in peace time.

From the CoC, one:

(2) Not to use information and communications technologies and information and communications technologies networks to carry out activities which run counter to the task of maintaining international peace and security.

From USG, two:

Acts of aggression are not permissible. And countries that are hurt by an attack have a right to respond in ways that are appropriate, proportional, and that minimize harm to innocent parties.

No country should seek either to prevent emergency teams from responding to a cybersecurity incident, or allow its own teams to cause harm.

From the UNGGE, one:

k. States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams of another State (sometimes known as CERTS or CSIRTS). A State should not use authorized emergency response teams to engage in malicious international activity.

From Tallinn, one:

9. A State injured by an internationally wrongful act may resort to proportionate countermeasures, including cyber countermeasures, against the responsible State.

From MSFT, three:

3. States should exercise restraint in developing cyber weapons and should ensure that any which are developed are limited, precise, and not reusable.

4. States should commit to nonproliferation activities related to cyber weapons.

5. States should limit their engagement in cyber offensive operations to avoid creating a mass event.

Analysis: Perhaps five years ago there was hope that cyberspace could remain “fundamentally a civilian space—a neighborhood, a library, a marketplace, a school yard, a workshop—and a new, exciting age in human experience, exploration and development.”[22] Today, with dozens of nations building offensive cyber capabilities, such a hope seems naïve. A non-weaponized cyberspace is unlikely. In the non-cyber world, the Proliferation Security Initiative[23] calls upon participating countries to interdict WMD related materials, especially if that state’s ports or infrastructure is being used to facilitate the transport and proliferation of WMD materials. In the text supporting its proposed norm 4 (nonproliferation), Microsoft calls on states to collaborate “with international partners and, to the extent practicable, private industry,” noting that such collaboration would “help reduce the possibility that cyber weapons could be used by non-state actors.”

[22] See: Jane Holl Lute and Bruce McConnell, “Op-Ed: A Civil Perspective on Cybersecurity,” *Wired,* February 14, 2011, http://www.wired.com/2011/02/dhs-op-ed/.

[23] See: http://www.psi-online.info/. Some have suggested that something like the PSI might work in cyber.

Preliminary Conclusions

1. There is considerable superficial convergence in norms, both in the general principles (Category I) and in particular areas such as mutual assistance (Category IV). This is a promising development, suggesting that where there is emerging agreement there is the possibility of more immediate and practical progress.
2. Serious areas of disagreement also remain; notable among them are different views as to the appropriate limits of state sovereignty, stemming in substantial part from cultural, political and military factors.
3. Relatedly, the asymmetric distribution of cyber capabilities across states affects preferences and emphases on norms. In this guise, one might imagine that progress will be faster should there be a more equal distribution of necessary capabilities among actors.
4. Such equalization could be viewed as contrary to the emerging nonproliferation norm, with the potential destabilizing effect of increasing the militarization of cyberspace. Equalization, without significant progress on measures of restraint, is thus inadvisable. The lack of attention to such measures in most of the documents reviewed is disappointing, and it undermines the commitment to reducing tension and promoting stability. In addition to reducing the spread of cyber weapons, measures of restraint in action would provide additional avenues to enhancing peace in cyberspace. Such measures could include: non-aggression or no-first-use pledges; identifying assets that should not be attacked, particularly in peace time; and stronger work to help legitimate actors protect themselves and each other (thus raising the costs to attackers).

Table 1: Comparative Study of Emerging Norms of State Behavior Related to the Uses of Information and Communications Technologies to Commit Internationally Wrongful Acts

Generic Norm Type	Source of Detailed Norm	
	CoC	Kerry Seoul Speech, May 18, 2015
I. Basic principles ensuring the security and stability of global cyberspace	(1) To comply with the Charter of the United Nations and universally recognized norms governing international relations that enshrine, inter alia, respect for the sovereignty, territorial integrity and political independence of all States, respect for human rights and fundamental freedoms and respect for the diversity of history, culture and social systems of all countries. (7) To recognize that the rights of an individual in the offline environment must also be protected in the online environment; to fully respect rights and freedoms in the information space, including the right and freedom to seek, receive, and impart information, taking into account that [international law] attaches to that right special duties and responsibilities....[complete text in body of paper]	Acts of aggression are not permissible. And countries that are hurt by an attack have a right to respond in ways that are appropriate, proportional, and that minimize harm to innocent parties.
II. The responsibility of states to avoid and prevent certain types of cyber attacks launched from their territories	(2) Not to use information and communications technologies and information and communications networks to carry out activities which run counter to the task of maintaining international peace and security. (3) Not to use information and communications technologies and information and communications technologies networks to interfere in the internal affairs of other States or with the aim of undermining their political, economic and social stability.	No country should conduct or knowingly support online activity that intentionally damages or impedes the use of another country's critical infrastructure. No country should conduct or support cyber-enabled theft of intellectual property, trade secrets, or other confidential business information for commercial gain. Every country should mitigate malicious cyber activity emanating from its soil, and they should do so in a transparent, accountable and cooperative way.
III. The responsibility of states to enhance the security of information and systems within their territories	(5) To endeavor to ensure the supply chain security of information and communications technology goods and services.... (6) To reaffirm the rights and responsibilities of all States, in accordance with the relevant norms and rules, regarding legal protection of their information space and critical information infrastructure against damage resulting from threats, interference, attack and sabotage.	
IV. The duty of states to cooperate with each other to mitigate certain types of cyber incidents	(4) To cooperate in combating criminal and terrorist activities that use information and communications technologies and information and communications networks, and in curbing the dissemination of information that incites terrorism, separatism or extremism or that inflames hatred on ethnic, racial or religious grounds.	Every country should do what it can to help states that are victimized by a cyberattack.
V. Restraint in the development and use of cyber weapons in peace time	(2) Not to use information and communications technologies and information and communications technologies networks to carry out activities which run counter to the task of maintaining international peace and security.	Acts of aggression are not permissible. And countries that are hurt by an attack have a right to respond in ways that are appropriate, proportional, and that minimize harm to innocent parties. No country should seek either to prevent emergency teams from responding to a cybersecurity incident, or allow its own teams to cause harm.

Source of Detailed Norm		
UNGGE on Information Security, Aug. 2015, Sec. 13	Tallinn Manual on the International Law Applicable to Cyber Warfare	Microsoft Paper: "International Cybersecurity Norms," Dec. 2014
a. Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security. e. States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression.		
c. States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs. f. A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public.	5. A State shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States.	
g. States should take appropriate measures to protect their critical infrastructure from ICT threats…. i. States should take reasonable steps to ensure the integrity of the supply chain so end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions. j. States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure.	1. A State may exercise control over cyber infrastructure and activities within its sovereign territory. 2. Without prejudice to applicable international obligations, a State may exercise its jurisdiction: (a) over persons engaged in cyber activities on its territory; (b) over cyber infrastructure located on its territory; and, (c) extraterritorially, in accordance with international law.	1. States should not target ICT companies to insert vulnerabilities (backdoors) or take actions that would otherwise undermine public trust in [commercial] products and services. 2. States should have a clear principle-based policy for handling product and service vulnerabilities that reflects a strong mandate to report them to vendors rather than to stockpile, buy, sell, or exploit them.
b. In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences. h. States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty.		6. States should assist private sector efforts to detect, contain, respond to, and recover from events in cyberspace.
k. States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams of another State (sometimes known as CERTS or CSIRTS). A State should not use authorized emergency response teams to engage in malicious international activity.	9. A State injured by an internationally wrongful act may resort to proportionate countermeasures, including cyber countermeasures, against the responsible State.	3. States should exercise restraint in developing cyber weapons and should ensure that any which are developed are limited, precise, and not reusable. 4. States should commit to nonproliferation activities related to cyber weapons. 5. States should limit their engagement in cyber offensive operations to avoid creating a mass event.

Appendix II

It is useful to be clear about assumptions about norms in cyberspace. As suggested by Keohane and Victor, even some of these assumptions may be contested. Table 1 offers an indicative list of such assumptions that could be informing state action.

ASSUMPTIONS ABOUT THE TERRAIN OF NORMS IN INTERNATIONAL LAW

1. Discussions are often confounded by loose usage of the term “norms” which has several meanings depending on the context (international legal norms, domestic legal norms, moral norms, political norms, professional norms, business norms and so on).
2. An international legal norm can be one that is universally agreed upon (with universal application) or one limited to a group of consenting states (applying only to the consenting states).
3. New international legal norms with universal application usually take decades (if not a century or two) to develop and become accepted as norms.
4. Norms are often constituted by “regimes” (of practice) that subsequently become legal norms.
5. Normative behaviors (such as consultation, self-restraint and dispute resolution by peaceful means) can be adjuncts to or even substitutes for norms.
6. Practices unregulated by norms coexist with emerging norms, universally accepted norms and contested norms.
7. Politics, like diplomacy, is a contest over the right to dictate norms or to at least have the upper hand in shaping norm development or shaping an argument about how to interpret and implement existing norms.

ADDITIONAL ASSUMPTIONS ABOUT THE NORMATIVE TERRAIN OF CYBERSPACE

1. Cyberspace is ubiquitous and highly variegated: norms, laws and contested practices of cyberspace are also ubiquitous and highly variegated.
2. Some examples: IPR law, trade law, investment law, labor law, human rights, state responsibility, diplomatic (sovereign) immunity, Law of the Sea, air and space, air traffic control, disaster relief, pandemic control, LOAC, private international law, extradition treaties, non-aggression treaties.
3. States are only one category of actor in cyberspace, and they no longer have a monopoly on determining norms.
4. Ethical and political contest over the meaning of existing or emerging norms is severely magnified and exaggerated at all levels by netizen power and private sector power.

Table 1: Indicative List of Assumptions about the Normative Terrain of Cyberspace[24]

[24] See: Greg Austin, “China’s Position on Norms in Cyberspace,” NATO Cooperative Cyber Defence Centre of Excellence Cycon Paper, 2015, in publication as part of an edited volume edited by Anna-Maria Osula.

Appendix III

Lessons from the EastWest Institute as a Model or Foundation

Since 2009, the EastWest Institute has been involved in some way in international regime formation for cyberspace. The work has varied in that period, from a focus on breakthroughs in individual areas of international cyber policy (e-signatures, spam, priority communications, supply chain integrity) to promotion of stability in inter-state relations on big issues of war, peace and diplomacy involving Russia, China and the United States. We always saw the two broad dimensions as linked, with progress on more concrete business and community issues contributing to the building of confidence and trust among states. To this end, EastWest has consistently partnered with leading governments, businesses and civil society groups in our cyberspace work. It is our experience, documented extensively elsewhere, and confirmed by the sustained engagement of many parties in a range of non-governmental efforts, that much needs be done, more effectively and more rapidly, to bring stability, order and security to many aspects of cyberspace activity while preserving and promoting its economic and social benefits. Table A-1 provides a list of our policy papers in support of this work.

- *The Cybersecurity Agenda: Mobilizing for International Action* (2010)
- *Global Cyber Deterrence* (2010)
- *Rights and Responsibilities in Cyberspace: Balancing the Need for Security and Liberty* (2010)
- *Russia, the United States, and Cyber Diplomacy: Opening the Doors* (2010)
- *Protecting the Digital Economy* (2011) (2010 Summit Report)
- *Working Towards Rules for Governing Cyber Conflict: Rendering the Geneva and Hague Conventions in Cyberspace* (2011) (Russia-U.S. Working Group)
- *Fighting Spam to Build Trust* (2011) (China-U.S. working group)
- *Critical Terminology Foundations* (2011) (Russia-U.S. working group)
- *Mobilizing for International Action* (2011 Summit Report)
- *Priority International Communications* (2012)
- *Cyber Détente between the United States and China* (2012)
- *Critical Terminology Foundations 2* (2014) (Russia-U.S. working group)
- *A Measure of Restraint in Cyberspace: Reducing Risk to Civilian Nuclear Assets* (2014)
- *Resetting the System: Why Highly Secure Computing Should be the Priority of Cybersecurity Policies* (2014)
- *Convicting More Cyber Criminals* (2015)
- *Exploring Multi-Stakeholder Internet Governance* (2015)

Table A-1: List of EastWest Policy Reports and Discussion Papers

The work agenda for any new forum should probably be shaped by the original principle guiding the work of EastWest. The most influence on stakeholders can be achieved through the completion of showcase agendas for changes in specific sub-fields in a reasonably short time, while maintaining a broad dialogue with stakeholders globally for legitimacy, feedback and guidance.

EastWest Institute

Global Cooperation in Cyberspace Initiative

EastWest
INSTITUTE

SUPPORTERS

Microsoft
Huawei Technologies
Palo Alto Networks
NXP Semiconductors
Qihoo 360
Unisys
CenturyLink
The William and Flora Hewlett Foundation

PARTNERS

IEEE Communications Society
Internet & Jurisdiction Project
Munich Security Conference
The Open Group
The University of New South Wales

Building Trust Delivering Solutions

The EastWest Institute works to reduce international conflict, addressing seemingly intractable problems that threaten world security and stability. We forge new connections and build trust among global leaders and influencers, help create practical new ideas, and take action through our network of global decision-makers. Independent and nonprofit since our founding in 1980, we have offices in New York, Brussels, Moscow and Washington. Learn more at **www.eastwest.ngo**.