An Augmented Summary

of

The Harvard, MIT and U. of Toronto

Cyber Norms Workshop

October 19-21, 2011
Cambridge, MA

by

Roger Hurwitz
Computer Science and Artificial Intelligence Laboratory, MIT
Canada Centre, Munk School of Global Affairs, U. of Toronto

rhhu@csail.mit.edu

May, 2012

WORKSHOP SPONSORS

Canada Centre for
Global Security Studies

BELFER CENTER
for Science and International Affairs

Explorations in Cyber International Relations
Massachusetts Institute of Technology Harvard University

MUNK
SCHOOL
OF
GLOBAL
AFFAIRS

MACARTHUR
The John D. and Catherine T. MacArthur Foundation

UNIVERSITY OF
TORONTO

Microsoft®

CSAIL

MIT

VE RI TAS
HARVARD

Executive Summary

The cyber norms workshop, Oct. 19-21, 2011, at MIT in Cambridge, MA, brought together cyber policy makers, cyber policy analysts, cyber security practitioners, and academics.[1] The workshop was inspired by the 2010 United Nations recommendation that nations discuss behavioral norms for cyberspace whose observance by state actors would reduce the risks of misunderstanding and conflict. The workshop's organizers hoped that it would generate informed views on the contents of such norms and thereby support discussions among governments in response to the call. Accordingly, a preliminary report on the workshop was completed immediately afterwards and submitted to the organizers and some participants of the London conference intergovernmental conference on cyber norms, held two weeks later (Nov. 1-2, 2011).

This follow-on report is an opportunity to take a somewhat broader look at the needs for and roles of cyber norms that will be accepted and observed by a broad international community. While heavily based on the discussions at the workshop, the report also draws upon some work, comments and reflections on cyber norms that were not referenced then or only available later. This makes the report more timely and forward looking, but less a proceedings or summary. Consider it a statement by the author, one of the principal organizers, of principal points made in the workshop, with the hope their consideration by others contributes to the development of cyber norms. Furthermore, these points should no way be regarded as recommendations or consensus of the workshop participants, especially since there was no consensus finding process at the workshop. Because the workshop was conducted under the Chatham rule, the points, however, are not attributed to specific participants who raised and commented upon them.

The discussions focused on six areas of concern for cyberspace: a) military operations; b) political, military and economic espionage; c) cybercrime; d) development of underlying technologies and supply chain management; e) public-private partnerships; f) global information society and Internet freedom. Proposed norms were discussed with regard to how their observance would serve one or more of several purposes:

- Foster a common understanding of the intents and acceptability of cyber behaviors, thereby reducing risks of misunderstandings, conflicts and escalation at the interstate level;
- Provide safe, secure use of cyberspace by individuals and organizations, thereby assuring continued social and economic benefits of cyberspace for societies;
- Guide beneficial development of cyber technologies and applications.

Participants also evaluated the proposals according to how practicable they were and how broadly they would be accepted. It was noted that some norms, like the unfiltered flow of political information, would not be accepted by all states, but would nevertheless be promoted among like-minded states. Thus, the workshop also recognized current and emerging differences of normative regimes for cyberspace at the international level.

[1] For agenda, participants, framing questions and preliminary report, see http://www.citizenlab.org/cybernorms/.

The following were prominent among proposals, which appeared most likely to gain wide acceptance and contribute significantly to the stability, security or development of cyberspace:

- States should distinguish between disruptive and damaging cyber attacks and evaluate a damaging attack on the basis of its scope, duration and lethality;
- States have a duty to assist other states that have suffer a major cyber attack or disaster, and also have a duty to inform others of new threats in cyberspace;
- States whose territories or citizens are involved in transborder cyber activities which are unambiguously criminal in their states should cooperate in the investigation of these crimes and the apprehension of their perpetrators;
- States should enable the formation of public-private partnerships for cybersecurity, which include both local and international ICT companies operating in their territories.

Acknowledgements and thanks

Sponsors: The Belfer Center for Science and International Affairs at the Harvard Kennedy School of Government; The Canada Centre for Global Security Studies and Citizen Lab at the University of Toronto's Munk School of Global Affairs; Explorations in Cyber International Relations (ECIR), a joint Harvard-MIT research project; Microsoft Corporation's Office of Global Security Strategy and Diplomacy (GSSD); MIT's Computer Science and Artificial Intelligence Laboratory (CSAIL); and The John D. and Catherine T. MacArthur Foundation;

My co-chair Prof. Joseph Nye and members of the organizing committee who shaped the agenda and the framing questions for the discussion panels;

The participants who made the workshop a stimulating exchange of information, insights and ideas.

The note takers Camino Kavanagh, Tim Maurer and Michael Sechrist

Preparation of this summary was partly funded by the Office of Naval Research under award number N000140910597. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the author and do not necessarily reflect the views of the Office of Naval Research or any of the people and organizations mentioned above.

1. Introduction

The cyber norms workshop at MIT, October 19-21, 2011, brought together government officials involved with cyber security and defense policies, independent policy analysts, cyber security practitioners, technologists, and scholars of international norms and national security policies. Its purpose was to identify possible norms whose diffusion and observance by states could reduce instability and insecurity in cyberspace and help guide its development. The workshop was inspired in part by the UN General Assembly's approval, in 2010, of a recommendation by a group of governmental experts on information security that states "discuss norms pertaining to State use of ICTs, to reduce collective risk and protect critical national and international infrastructure."[2] The workshop organizers believed the participants would produce informed views on the contents for such norms that might subsequently support discussions among governments in response to the recommendation. Accordingly, a preliminary report on the workshop was submitted to the organizers and some participants of the London conference intergovernmental conference on cyber norms, held two weeks later (Nov. 1-2, 2011).[3]

This report is a further effort to communicate the principal discussions of the workshop, but it also draws upon some work, comments and reflections on cyber norms that were not referenced then or only available later. This makes the report more timely and forward looking, but not a "proceedings". It is an augmented summary by the author, a convener of the workshop, of principal points he believes were made there. Furthermore, these points should not be regarded as recommendations of the workshop or a consensus of its participants, for apart from the later elaborations, there was by design no consensus finding process at the workshop. However, the points, are not attributed to specific participants who raised and commented upon them. because the workshop was conducted under the Chatham rule,

The report is divided as follows. The next section first makes general comments on the roles and bases of norms in international relations. Then it describes the conditions that prompted the UN recommendation, namely a growing crisis of cybersecurity, on one hand, and, on the other hand, dramatic changes in cyber demographics that challenge the privilege of traditional Internet culture and institutions for "the way of doing things." The third section recapitulates workshop discussions of norms that were proposed for six areas of cyber related behavior: a) military operations; b) political, military and economic espionage; c) cybercrime; d) development of underlying technologies and supply chain management; e) public-private partnerships; f) global information society and Internet freedom. This section also goes beyond the discussions by trying to prioritize the proposed according to their possible amelioration of conditions in cyberspace, the feasibility of their being accepted and their technical practicability. The final section selects several proposals which the international community would do well to consider now, and it concludes by noting that even broadly accepted norms are just part of the solution for security in international cyberspace.

[2] United Nations General Assembly A/65/201; 7/30/2010. http://unidir.org/pdf/activites/pdf5-act483.pdf (retrieved 2/1/2012).

[3] For the preliminary report, agenda, participants, and framing questions for the panel discussions, see http://www.citizenlab.org/cybernorms/. The preliminary report was on the basis of notes taken by Camino Kavanagh, Tim Maurer and Michael Sechrist.

2. International Norms and Cyberspace

Norms are shared expectations about appropriate behavior. They may either be descriptive of current practices, or prescriptive, that is, specify behaviors, which those accepting the norm demand of one another. A prescriptive norm thus creates a challenge of moving those who accept it from their current practices to the expected behaviors. This process might be achieved through incentives or sanctions, with the provision of these itself becoming an extension of the norm, e.g., "humanitarian intervention" on behalf of human rights. International norms are distinct from laws or contractual provisions, although they might be subsequently articulated in such instruments, but they are stronger than standards for "voluntary compliance." At the very least, acceptance of a norm by a state puts the state's reputation at risk. If it fails to follow the norm, other states which accept that norm, will typically demand an explanation or account, rather than ignoring the violation or dismissing it as self- interested behavior.

There are several utilitarian reasons why governments accept international norms, which may at times constrain their freedom of action. First, norms help solve planning and coordination problems by specifying appropriate actions in particular situations, so agents know what actions they are expected to take and the likely response to them. In this way, norms reduce the variability, hence increase the predictability, of situational outcomes. Second, in many instances observance of a norm resolves collective action problems, which occur if actions taken according to their short-term self-interests will produce a less than satisfactory collective outcome. In this respect, the norm is an efficiency engine and also reconciles the long term interests of the state with the current choice. A less self-interested reason for a state to advocate and observe certain norms is they support values to which the state is committed, e.g., protection of human rights. Also a state might adhere to a norm for partly symbolic reasons, despite the political or economic costs. That is, other states with greater prestige have adopted the norm, so the state's adopting it would enhance its status, e.g., cooperation with the International Criminal Court for prosecution of war criminals. Conversely, a state might choose to assert its independence of other states with regard to certain matters by rejecting a norm or institutional practice these other states favor. Arguably, this is one reason why China demands an alternative to ICANN for oversight of the Internet.

The current willingness of states to discuss international norms for cyber behaviors a utilitarian notion of norms and responds to a common, growing sense among leaders and publics of insecurity and threats in cyberspace. The 2010 UN resolution expressed concern that the lack of "shared understanding regarding international norms pertaining to state use of ICT's risked misperceptions and "could affect crisis management in the event of major incidents," i.e., trigger escalations. It recognized

> the need for international cooperation against threats in the sphere of ICT security in order to combat the criminal misuse of information technology, to create a global culture of cybersecurity and to promote other essential measures that can reduce risk…

and added

> it is obvious that no State is able to address these [cyber] threats alone. Confronting the challenges of the twenty-first century depends on successful cooperation among like-minded partners. Collaboration among States, and between States, the private sector

> and civil society, is important and measures to improve information security require broad international cooperation to be effective.[4]

The threats noticed at that time included cybercrime, cyber attacks on critical infrastructure (DDoS, Stuxnet-type malware), political and industrial espionage, cyber-enabled terrorism, widespread restrictions (censorship, filtering) of Internet use, and the proliferation of the means to achieve all these. By the following year, viewing the effects of the "Arab spring," some countries would add to that list the cyber-fueling of anti-regime protests and implicitly respond to it in proposing codes for international cyber behavior.[5] Many states saw the threats as challenges to their national security and to the beneficial roles of the Internet and other cyber technologies in their social and economic development. So the UN resolution spoke to a common interest as well as need for international cooperation to control these threats – for actions and restraints which could be partly specified in norms.

The explosive growth of Internet usage and applications, the rise of mobile computing, and the demographic changes associated with these are also background conditions for proposals and discussions of international cyber norms. This growth has far outstripped already limited cyber security capabilities; it has created many new targets for attacks and exploits, vastly more online vulnerabilities and near countless naïve users. The global penetration of the Internet has changed its demographics over the past decade, from 200 million users concentrated in North America and Western Europe countries to over 2 billion, with the plurality located in the East and South -- in countries where governments traditionally controlled public discourse, tightly regulated communications and dominated the private sector. One consequence has been pushback by state and frequently religious authorities against the regnant Internet norms of openness and free speech and against the multi stakeholder approach to Internet administration, planning and development.[6]

Aware of these differences, the workshop participants tended to a more expansive view of the purpose for cyber norms than that in the UN resolution. Many agreed that desirable **cyber norms should aim to assure that "all [states, organizations, individuals] will exercise stewardship [of cyberspace], domestically and internationally, to sustain and advance prosperity, knowledge, well being and the global good."** An alternative, equally accepted formulation of the goal was "a trusted and secure global environment to sustain (peaceful) commerce, communications, international peace and security." The discussion on this point noted that the development of norms consistent with the goal can draw upon a considerable body of custom, laws and practices pertaining to international spaces, e.g., air, sea, and activities within them, e.g., war, trade. Cyber norms might therefore be interpretations of existing international norms for cyberspace, and determining their limitations. For example, states could use the rights of passage in commons, like international airspace and the oceans, as a basis to expect no interference with their government and military electronic

[4] United Nations General Assembly A/65/201; 7/30/2010. http://unidir.org/pdf/activites/pdf5-act483.pdf (retrieved 2/1/2012).

[5] Most notably, the Russian draft for a "Convention on international information security," presented to the "International meeting of high-ranking officials responsible for security matters," Ekaterinburg, Russia, Sept. 21-22, 2011.

[6] R. Deibert & R. Rohozinski, Contesting Cyberspace and the Coming Crisis of Authority, in R. Deibert et al., *Access Contested: Security, Identity and Resistance in Asian Cyberspace* (Cambridge, MA: MIT, 2011), 21-41.

communications in its hops through other countries.[7] On this view, the creation of norms that are novel and cyber specific will depend on encountering practices or incidents where the extension to cyber of norms in other domains produce results that many will consider too limited and unsatisfactory. For example, requiring that a cyber attack destroy property, say like Stuxnet, to be considered an armed attack, is arguably too narrow a definition, when a DDoS or sensor poisoning of cyber based critical infrastructure installations might cause as much devastation and suffering as kinetic attacks on the installations.[8] A focus among international legal scholars, academics and government cyber policy makers on just these situations might facilitate the formulation, diffusion and acceptance of a common set of norms for when the technologies make a difference.

Even that, however, might be too ambitious a goal, especially given the many distinct contexts in which ICT security and integrity are key, e.g., war, domestic security, economic, political and social interactions. States today differ in their visions of cyberspace, especially with regard to issues of information access, sovereign authority and sovereign responsibilities. Also, they do not similarly rank the threats or even have the same sets for ranking. China and Russia construe the flows of dissident political information – Internet Freedom, by another name – as a threat and are less concerned than the U.S. about industrial espionage. Consequently, there might be little agreement on where to begin and the specification of norms might be slow and piecemeal. Indeed, this outlook is supported by the evident ideological differences in the controversies surrounding the few existing cyber specific international agreements, most notably the Budapest Convention on Cybercrime, but also, the Shanghai Coordinating Organization (SCO) on information security.

The workshop participants therefore noted that **a state might have different expectations regarding another state's cyber relevant behavior at bilateral, minilateral – say, among allies -- global levels.** States generally would share a minimal set of expectations for cyber related behaviors, but the set would become more demanding in alliances, regions or other clusters and again more demanding and specific within certain bilateral relations. The contents of the expectations would be different for different clusters and bilateral relations. A signatory to the Budapest Convention might share information for computer forensics only with other signatories and expect that only signatories will share with it. Similarly, China should expect that only other SCO members will suppress dissident information flows from servers in their territories. The United States and New Zealand might expect cooperation from each other in matters of special interest to one of them, such as the suppressing the distribution of allegedly pirated material.

A important question is whether the minimal set could be sufficiently robust to prevent fragmentation of the Internet into competing normative regimes. According to some workshop participants the crafting of norms in it should be guided by these principles**:**

- Cyberspace should remain open, interoperable and reliable;
- All nations have an interest in a clean, healthy cyberspace, and consequent to that interest, they have a duty to assist, inform and educate one another;
- All nations have an interest in a cyberspace that retains the trust of its users;
- Fundamental freedoms of people for information and connectivity need be upheld;

[7] A. Denmark & J. Mulvenon, eds., "Contested Commons: The Future of American Power in a Multipolar World," Washington, Center for a New American Security, 2010.

[8] M. Schmitt, Cyber operations and the jus ad bellum revisited. *Villanova Law Review*, 56 (2011), 569-605.

- Key international laws, norms, and rules should be extended to cyberspace;
- Multi-stakeholder stewardship, involving governments, international organizations and the private sector, should shape the development and maintenance of the Internet;
- Governments should refrain from political interference in technical development and standards for the Internet.

Yet as suggested above, there is no agreement among states on all these principles or there relative importance. But fragmentation might not be inevitable, since it is common for states to observe an international norm without publicly endorsing it. This seems the case for some states with regard to their meeting in practice most provisions of the Budapest Convention. In other words, the articulation of a cyber norm and its practice by a small group of states can be effective in changing expectations and behaviors among other states.

3. Possible Cyber Norms

Following the UN resolution supporting the discussion of cyber norms, several countries and groups of countries have offered broad strategies or codes of conduct for more secure and stable international activities in cyberspace.[9] Despite each having some elements acceptable to all sides, e.g., assisting countries in developing cybersecurity policies and capabilities, the discussions about them have tended to sharpen the differences among countries, particularly over issues of governance and freedom of information. One lesson from this may be that states should avoid grand plans for international cybersecurity, but instead work on norms in areas where their current practices have been mutually acceptable or where they have expressed strong interests for cooperation. The workshop results can support that tack, since the workshop evaluated prospective norms on their respective merits rather than as parts of a comprehensive program. Table 1 presents the norms that attracted the most interest (but these table should not be viewed as a consensus, since any consensus seeking process was deliberately avoided).[10]

To be sure, like the principles listed above, the tabled norms tend to reflect a western vision of how cyberspace should be constructed, since workshop participants came only from the US and its allies. Yet the decomposition of cyberspace into issue areas enabled participants to evaluate the ripeness of facets of cyber behavior for formalization and the readiness of governments to accept the formulas as norms. Where possible, the proposed norms are distinguished to whether they articulate principles for cyberspace, including norms for dealing with states of exception, like conflicts, or recommend best practices and operating rules.

[9] Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, A/66/39. http://blog.internetgovernance.org/pdf/UN-infosec-code.pdf; the Russian draft for a "Convention on international information security" (Ekaterinburg); White House, International strategy for cyberspace: prosperity, security and openness in a networked world. May, 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf; BSA Multistakeholder meeting on global Internet governance, Sept. 1-2, 2011, Recommendations. http://www.culturalivre.org.br/artigos/IBSA_recommendations_Internet_Governance.pdf;

[10] Table 1 is based on C. Kavanagh, Wither "rules of the road" for cyberspace? CyberDialogue2012, March 18-19, 2012, Toronto, Canada. http://www.cyberdialogue.ca/briefs/

Table 1: Possible norms tabled at a workshop hosted by Harvard Kennedy School Belfer Center, MIT CSAIL, & U. of Toronto's Canada Centre for Global Security Studies

Military operations in cyberspace	Political, military, and economic espionage	Cybercrime	Technological foundations & supply chain	Public-private partnerships/ defensive coordination	Internet freedom global information society
In principle, apply LOAC to military responses and operations	Banning of large-scale commercial espionage which could be promoted as a universal customary norm to multiple international bodies and incorporated in bilateral relations.	Norm to ensure states & other stakeholders educate themselves on cybercrime, including with respect to the hiring of criminal hackers.	States should recognize the international implications of their technical decisions, and act with respect for one another's networks and the broader Internet	Governments should seek cooperation with the private sector to assure a clean and healthy Internet.	Promote Internet freedom as a global norm, but allow for ambiguity reduce friction regarding the standards of Internet freedom
Confidence-building measures such as cyber hotline, greater differentiation of cyber incidents, establishing mechanisms for crisis management & de-escalation	Regulate trade in espionage and surveillance services by defense contractors in developed countries to authoritarian countries for use vs. political dissidents	Distinction between low & high impact criminals and expectations for cooperation in the pursuit of high impact criminals.	States should act within their authorities to help ensure the end-to-end interoperability of an Internet accessible to all.	Norm that limits or calls for arrangements that limit (or specifies circumstances for) surveillance and data collection by private companies	
A structural norm (practice) of military involvement in the protection of domestic critical infrastructure from cyber attack	Encryption of computers and cloud servers to inhibit theft of politically sensitive information (a la Wikileaks)	Data retention & transborder accessibility for high impact crime	Respect the free flow of information in national network configurations; no arbitrary interference with internationally interconnected infrastructure		

Military operations in cyberspace	Political, military, and economic espionage	Cybercrime	Technological foundations & supply chain	Public-private partnerships/ defensive coordination	Internet freedom global information society
Norms to routinely share information, assist in disaster or attack, cooperate in forensics, collaborate in analysis of attacks	Duty to warn & duty to assist. Analogies to mandatory notification should be institutionalized at the international level in data sharing procedures among CERT's and NATO allies		Globally accepted norms and standards to assure cyber supply chain, including third-party certification of production centers, third-party assurances of hardware and software, a certification architecture enabling trusted chains of custody for components		
	Letters of marque, issued by states to license private parties to pursue cyber spies		"naming and shaming" of insecure producers, and barring their sales to government and defense sectors.		

Military operations: Existing international laws specify neither the types of cyber operations which a targeted country could legitimately consider grounds for war (*ius ad bellum) n*or the constraints on cyber operations a country needs to observe in war (*ius in bello*). Governments have avoided specifying redlines whose crossings would provoke them to retaliation, including armed response, for fear that would effectively license adversaries to mount less injurious operations. This reluctance is understandable and consistent with deterrence theory, which argues that the possibility rather than the certainty of retaliation is sufficient to give an adversary pause before an attack.[11] However it leaves the international community without shared expectations as to the limits of peacetime cyber behaviors, on one hand, and responses from countries subject to attacks, on the other. The uncertainty is compounded by the abilities of non-state actors to mount serious cyber attacks on one state from the territory of one or more states, and by the absence of norms, which hold states responsible to prevent such attacks.

The short history of international cyber conflict provides few landmarks for this uncharted area. The 2007 DDoS attack on Estonia did not provoke retaliation from Estonia's NATO allies, although according to some reports Estonia did ask for some response under Article 5, the collective security provision, of the NATO treaty. With that attack in mind, an advisory group in 2010, recommended that NATO's new strategic doctrine specify that transborder cyber attacks on a member state would ordinarily trigger consultations (Article 4) and certain attacks might even warrant a response under Article 5.[12] NATO, however, passed on this recommendation, preferring a policy of deciding the appropriate response on a case by case basis. Similarly, the DDoS attacks on American government sites apparently did not warrant retaliation, even had the government been able to attribute them to a state actor with a reasonable confidence. (Although the North Korean military or security service was suspected to have launched the attacks, they were originally controlled from South Korea, then from US and European sites, with little evidence of a North Korean link.) The Stuxnet attack, which damaged rather than just disrupted Iranian facilities, generated no overt response from the Iran, not even a complaint against unknown, presumably state, actors for endangering international security. Iran's leaders, of course, had their reasons for not responding: any complaint would draw more scrutiny to their nuclear program targeted by the attack and reveal more vulnerability of their facilities. Other governments were also silent, some perhaps having been complicit in the attack, and many, no doubt, applauding its sabotage of the Iranian nuclear program.

The lack of forceful responses by the victims in these episodes may indicate a common uncertainty about the gravity of cyber attacks and a reluctance to extend, possibly escalate, a conflict over them. States might not be bluffing when they declare a right to respond to cyber attacks by any means, but in practice they seem either to have no clear redlines or, if they do, no attacks, so far, have crossed them. Scholars of international law and other observers have addressed this void with greater certitude, with at least one characterizing the disruption of critical infrastructure in Estonia as rising to the level of "armed attack."[13] Others set the bar higher, at Stuxnet-like attacks with the potential to destroy infrastructure like nuclear reactors and produce very lethal results. In their opinion, these now apparent possibilities should prompt

[11] T. Schelling, *The Strategy of Conflict*. Cambridge, MA: Harvard,1(960) 1981.

[12] R. Wall, NATO urged on missile and cyber-defense. *Aviation Week*. May 18, 2010. http://www.aviationweek.com/aw/generic/story.jsp?id=news/asd/2010/05/18/02.xml&channel=space

[13] M. Schmitt, Cyber operations and the jus ad bellum revisited. *Villanova Law Review*, 56 (2011), 569-605.

states to agree to prohibit certain types of attacks and to provide remedies for them, such as the right of a state under cyber attack to get assistance from other states.[14]

This recommendation is not far-fetched, especially if, absent generally accepted redlines, national security officials evaluate cyber attacks cases by case and weigh responses to them with the traditional criteria for evaluating kinetic attacks, viz., scope, duration and lethality. Applied to cyberspace, these criteria would distinguish between disruptive and damaging attacks, and restrain military responses to the disruptive ones. Talks that affirmed the applicability of these criteria could get broad support from states and reduce the threat of escalation from relatively minor disruptive attacks. Adoption of these criteria would not rule out the use of force in response to damaging attacks, but the talks could help create a bias against it by advocating several norms, with potential for widespread acceptance, that would mitigate the damage and help identify parties responsible for the attacks. These include the notion of e-SOS or "duty to assist," that requires states to offer help to a state whose cyber-based infrastructures were damaged, a related duty of states to inform others of malware threats they have discovered, cooperation in forensics, and a commitment to seek mediation for cyber related conflicts.

Cyber powers, with the exception of China, agree that LOAC should apply to cyber conflicts. However, participants at the workshop expressed some concern that developing rules of engagement based on LOAC principles of proportionality of response, avoidance of civilian targets and minimization of ancillary casualties, may prove difficult. There is little experience of cyber attacks in war-like contexts and insufficient knowledge of their consequences. While, according to the cliché, the damage done by a bomb of a particular size is well-known, that for cyber attack on a military network or critical infrastructure is not. It can depend as much on the configuration of the target's networks as on the intended scope of the attack. Moreover cyberspace does not easily afford the distinctions upon which rules of engagement for "meat space" rely, viz., military vs. civilian, attack vs. espionage, state vs. non-state agents, intentional vs. accidental. For example, the US military uses civilian networks in over 90% of its communications, and the figures are probably similar for other militaries. Although international dialogue has begun about measures that might sharpen the distinctions, e.g., digital equivalents of insignia, on packets to indicate their military or humanitarian content, many points need be addressed.[15] Also for such dialogue to reach results that are applicable to future cyber conflicts, states will need to disclose some of their cyber offensive capabilities and plans for using them.

In view of the continuing ambiguities regarding causes and conduct of war in cyberspace, the workshop discussion emphasized the desirability of confidence building measures, e.g., a cyber

[14] For example, D. Hollis, Could deploying Stuxnet be a war crime? *Opinio Juris,* Jan. 25, 2011. http://opiniojuris.org/2011/01/25/could-deploying-stuxnet-be-a-war-crime/. "conditions cry out for (a) states to devise specific rules for launching or defending against cyber exploitations and cyber attacks; and (b) adopting an e-SOS as a first principle for mitigating or avoiding the most severe cyber threats. I don't think such rules would necessarily mean states could never deploy a Stuxnet (or that Iran would have an absolute right to issue an e-SOS if they did so). Rather, I think states themselves will have to devise the specific contours of acceptable (and unacceptable) behavior in cyberspace and, then defend their own acts on such terms. Without those rules, I worry that the very technology that we have welcomed for its transformative effects on our everyday lives may generate new forms of death and destruction for which the Stuxnet episode is merely an opening act."

[15] K. Rauscher & A. Korotkov, Working Towards Rules for Governing Cyber Conflict: Rendering the Geneva and Hague Conventions in Cyberspace. EastWest Institute, January, 2011.

hotline, greater differentiation of cyber incidents, and mechanisms, like third party mediation, for crisis management and de-escalation**.**

Two other military-related issues can concern strategies that seek to stabilize cyberspace by promoting appropriate norms: the responsibility of states for attacks originating in their territories, perpetrated by non-state actors and the involvement of military units in protecting of domestic critical infrastructure from cyber attacks. Acceptance of a norm that held states responsible for such attacks would be consistent with current international law for kinetic attacks, with the UN efforts to foster a worldwide culture of cyber security and with efforts to curtail certain states' use of proxies. However there might be difficulty in reaching agreement on the appropriate norm because of the various current suggestions as to what cyber attacks rise to a hostile act or armed attack. Some commentators who consider the 2007 DDoS attack on Estonia an armed attack emphasize the mental anguish Estonians suffered because of disrupted online services. Since authoritarian governments consider dissident political speech to disturb their countries' social stability, they could plausibly argue that under this definition, other states that allowed dissidents to communicate from their territories could be blamed for permitting "hostile acts" or "armed attacks." Hence, it might be sensible for the US and its allies to support a distinction between disruption and damage, before proposing a norm of sovereign responsibility for damaging attacks originating from a state's territory.

The U.S. and many of its allies are currently deliberating on the role that their respective militaries should play in defending from cyber attacks the critical information infrastructure, which serves their civilian populations. While some officials believe the militaries should take a lead role or a co-equal one with any civilian agency, because the militaries are better resourced and, noted above, depend on the infrastructures. Others are uneasy with the idea, because of its implications for the civil-military relationship in their states. Traditionally the militaries have been outward directed, with police and other security agencies responsible for internal protection. Also, giving the military a lead role in responding to an attack on the infrastructure could bias the conflict process toward retaliation and escalation, rather than resilience and recovery, because it introduces an offensive option. That prospect in turn raises the issue of appropriate rules of engagement when the attacker is a non-state actor.

Military, Political and Economic Espionage: The use of cyber technology for espionage raises questions about the current norms that permit espionage under international law but allow its prosecution under domestic law. This is because

- the technology allows the theft on secrets and intellectual property on an unprecedented scale;
- the spying at this scale is done remotely (electronically or digitally), leaving the victim with little in-domain recourse other than "naming and shaming" the perpetrator, i.e., no imprisonment or expulsion of captured spies;
- cyber systems used in espionage and other intelligence, surveillance and reconnaissance can blur the line between exploit and attack, causing damage and disruption as well as loss.

Given the traditional understanding of political and military espionage as needed for national security planning and preparation, proposals for their restriction would seem to have little chance of gaining traction. Nevertheless, because the scale of the cyber espionage may provoke aggressive responses from its victims, which in turn would destabilize the international system, some informal, unpublicized understandings might be reached on a bilateral basis as to an accepted level of espionage. In any case, the US and many of its allies will insist that industrial espionage by state actors is condemned by international law, since it is not motivated by a national security concern or part of anticipatory self-defense. The question is whether this espionage should be considered "economic warfare," which threatens international security, or more an unfair trade practice, which can be redressed by economic penalties. The latter view has the advantage of leading to the decomposition of the charges of espionage to individual cases or types of cases, with some dissipation of the grievance. That consequence can be important, since almost all the industrial espionage has been attributed to China, and its principal victim, the United States has progressed from annoyance to extreme irritation with China over its practice.

Can the US and like minded states effectively promote and sufficiently enforce a norm banning industrial spying, so that it might be eventually be widely accepted and followed? One model proposed for such an effort is the "proliferation security initiative" (PSI), in nations through bilateral and multilateral agreements have committed not to traffic in weapons of mass destruction and to act to interdict shipments of such materials. Adherence to the PSI grew from a core of eleven nations to nearly one hundred in less than a decade, despite controversy over the legality of interdiction on the high seas and opposition from China and many non-aligned nations, including India and Indonesia. For a comparable initiative on industrial espionage, the US and other interested countries would need laws enabling them to try in their own courts foreign nationals and companies for economic espionage originating outside their national boundaries. Prosecution of the same suspects by a number of states might both end the suspects' espionage and force the World Trade Organization to develop specific rules and remediation for industrial espionage that states could enact, e.g., damage awards against offending companies, tariffs against existing states. One major obstacle for this scenario is, in contrast to the PSI which spoke to the fears of many nations over WMD, only the United States and a few other states with major intellectual property stores are victimized by the industrial espionage. Consequently, gaining broader support would depend less on exemplary cases against the espionage, but on the expenditure of diplomatic and political capital – similar to the expenditures by advanced countries to get less developed ones to support their proposals for global copyright and patent protection. Moreover, the prosecutions of alleged spies, even under new enabling legislation, might prove difficult: many companies will shy at explicitly identifying what properties were stolen, while intelligence agencies may be reluctant to provide the evidence they have for fear of disclosing their sources or their own espionage activities. Galvanizing the international community against industrial espionage should be a goal for its victims, but without a compelling model for doing so, but its priority is open to question. More might be accomplished in serious bilateral talks between respective victims and perpetrators.

The workshop discussion on espionage acknowledged that enhanced cyber security awareness and hygiene at the enterprise level will do little to halt cyber espionage of any type. Because the incumbent cyber technologies are vulnerable, states and non-state actors will find ways to get to the targets of their choice. The value to their take, however, could be reduced by adherence to a norm at the operational level of end-to-end encryption or, failing that, encryption enablement of computers and servers that host politically or economically sensitive data. Enabling these practices should be one goal of international cooperation for capacity building in less developed countries.

An issue related to espionage is the surveillance (and censorship) by governments of their own citizens' online activities, often accomplished in less developed countries with technologies acquired from developed ones. For states that are committed to a global human rights agenda, such surveillance threatens the citizens' rights for information, expression and political association. One response has been proposals of norms among like-minded states that would impose or broaden existing export controls on the technologies. Such an initiative can prove effective quickly, because the technology suppliers are mainly in a small number of liberal democracies, where public opinion in support of such controls can be grown. In some cases, public reports that a company has supplied an obnoxious regime with such technology has already caused the company to claim it has or will stop the supply. As the operational level, however, there needs to be some distinction between "lawful" and "unlawful" use of the technologies, so that vendors will cooperate in enforcing the norms, rather than fear significant loss of sales.

Cybercrime: Strategies that promote international cooperation to combat cybercrime are vital for the stabilization and positive development of cyberspace. This is because cybercrime organizations breed new attack techniques, which can then be acquired by states, and the capabilities of these organizations, when augmented with outsourced specialized skills, can exceed those of almost all states acting alone. Yet a strategy that would focus on international cooperation for the apprehension and prosecution of cyber criminals now faces the choice of promoting the expansion of the Budapest Convention on Cybercrime or advocating a new treaty. The US and other supporters of the convention argue that it sets a standard for international cooperation in investigating and prosecuting cybercrime, notwithstanding having only thirty-one signatories over a decade. Critics complain fault the convention for being regional in character, deficient in provisions for handling data, and outdated by the new types of cyber crime, which have accompanied the exponential growth of Internet use, proliferation of mobile devices and the emergence of an Internet of things (devices).[16] They also note that many states in the East and South will not join the Convention because of its North Atlantic origins.

However a strategy that campaigns for either the old treaty or a new one might not be cost effective in reducing crime. There will be costs in trying to overcome the resistance that many states will have to joining. There are a variety of reasons for this resistance. Russia and some other states will not easily end policies of giving safe harbor to cyber criminals in return for their intelligence gathering and plausibly deniable offensive cyber operations, e.g., DDoS. Some states will be concerned about limits to their national sovereignty, changes in their criminals laws and procedures, or data retention practices that a new treaty or a revised Budapest convention will require.

Of course there are benefits from having a treaty, but the question is whether these might be realized in more cost effective ways. The benefits include standardizing investigatory procedures at an international level, harmonizing some laws across states and possibly retarding the growth of cybercrime in member states. Apparently a state's membership in the Budapest convention correlates with fewer cyber attacks originating from its territory than from a

[16] S. Schjølberg, Wanted: a United Nations cyberspace treaty. In A. Nagorski, ed., Global cyber deterrence: views from China, the U.S., Russia, India, and Norway. EastWest Institute, 2010, 11.

demographically comparable non-member state.[17] Perhaps the convention signaled to cyber criminals that the state would henceforth be more cybersecurity aware, so the criminals consequently launched their operations from more permissive places.

The promotion of norms which reduce either the vulnerability of users or the incentives for criminals could more easily produce similar effects on the levels of cybercrimes. These norms include information sharing and a duty to warn (or inform). The duty to warn or inform becomes increasingly relevant with the growth of situations where individuals, organizations or governments are unaware that a) their information systems are at risk, b) their data has been stolen or c) new organizational routines can produce new vulnerabilities. This duty has already been partially formalized at domestic levels by laws mandating notification of security breaches. It has begun institutionalization at the international level in data sharing procedures among CERT's and regional organizations of states, e.g., NATO. Cloud vendors and tier-1 ISPs, whose operations are not confined to any one state, should also be subject to such norms and laws, although there is no appropriate supervisory authority at this time. Because of their alignment with the UN resolution on cybersecurity, such norms can gain widespread acceptance, but will probably not become ubiquitous in practice. Some states and organizations will ignore these expectations due to their imposition of processing costs, reputational risks and disclosures of possible improprieties in data collection. Moreover, some old vulnerabilities will persist, new ones will be created and with them cyber crime. For that reason, a strategy should also deter cyber crime by promoting passive measures that interfere with criminals' getting their payoffs, e.g., blocking the ways that stolen information is monetized.

This approach, which emphasizes prevention over apprehension, does not preclude cooperation between members and non-members of the Budapest convention in the investigation of cyber crimes. It recommends rather than seeking a comprehensive framework for such cooperation, arrangements be developed in the context of bilateral relations, such as extensions where needed of mutual assistance treaties, or on a more informal, *ad hoc basis*. To that end, states, such as the US, which are zealous in the pursuit of cybercrime, will need to convince states like Russia and China that such cooperation is also in their interest, possibly by seeking cooperation only in cases of major criminality, e.g., terrorism, or regarding online activities that are unambiguously criminal in the respective jurisdictions, e.g., child pornography. Successful instances of cooperation in such cases can provide reusable routines and encouragement for more cooperation. Thus, China's Minister of Public Security said, after an unprecedented operation involving his police and the US FBI closed down a child pornography ring: "Although China and the U.S. have different judicial systems and cultural values, the two sides share a common view in crime-fighting," The Minister then pledged China would continue to strengthen its law enforcement cooperation with foreign countries and vigorously fight transnational illegal activities, especially crimes committed through the Internet.[18]

[17] S. Kim et al., A comparative study of cyberattacks. *Communications of the ACM*. 55:3, March 2012, 66-73

[18] Chinese police chief vows international cooperation in fighting Internet crimes. Xinhua, Aug. 30, 2011. http://news.xinhuanet.com/english2010/china/2011-08/30/c_131085036.htm. Unfortunately the FBI which initiated the investigation gave the Chinese police very little credit in its press release on the operation. By not appreciating the importance the Chinese attached to the cooperation, it missed an opportunity for building a relationship.

Technological Foundations: Today's cyber systems are vulnerable to attack and exploitation; tomorrow's will be even more vulnerable, since they will have more lines of code and more devices attached to them. As the attack surfaces multiply, attackers are innovating faster than defenders. So effective defense will require exponential gains in rate of defense innovation. For workshop participants who came from the industry and research communities, the following norms captured the appropriate roles for states in promoting the needed changes, as well as defending the existing Internet:

- States need to recognize the international implications of their technical decisions, and act with respect for one another's networks and the broader Internet
- States should act within their authorities to help ensure the end-to-end interoperability of an Internet accessible to all
- States should respect the free flow of information in national network configurations, ensuring they do not arbitrarily interfere with internationally interconnected infrastructure
- States should recognize and act on their responsibility to protect information infrastructures and secure national systems from damage or misuse

These norms accord with the principles of openness and security articulated in the "US International Strategy for Cyberspace," and with the idea that technologists make the technical decisions. In turn, their design decisions should

- Advance the common interest;
- Support the soundest technical standards;
- Be transparent, with regard to properties, rationale and metrics;
- Have no hidden vulnerabilities or trojans, and
- Aspire to minimal complexity, i.e., no unnecessary features that might introduce vulnerabilities.

Delivering on these expectations will be difficult amid current and foreseeable technological competitions, efforts to engineer network standards and computational frameworks for national advantage or more facile information filtering, industrial espionage and predatory trade practices in hardware. (Threat of) recourse to global organizations, e.g., WTO, or actions within bilateral relations leading to sanctions on bad actions will be needed for sound standards to prevail. The political costs for such actions can be justified on the grounds that since good ICT standards by reducing opportunities for bad cyber behavior, can contribute to international stability. On this view, the US and like-minded states from the technical communities in states that are less committed to these norms. However the technologists in those states have not yet or are just beginning to work with international bodies that have roles in developing cyberspace, e.g., IETF, or assuring its security, e.g., ISO. Also the technologists in some of these countries might not have the freedom to take positions which conflict with their governments' views.

Norms and standards to assure the integrity of the cyber supply chain must also be globally followed, since global distribution of production and open markets create ubiquitous risk. It is important that such expectations be shared widely among consumers so that there will be pressure on producers to satisfy them. Foreseeable operational norms or standard practices would involve third-party certification of production centers, third-party assurances of hardware and software, a certification architecture enabling trusted chains of custody for components, "naming and shaming" of insecure producers, and barring their sales to government and defense sectors. There might initially be a need for incentives or government pressure for large corporations on both the supply and consumer sides to enter such a system. Ultimately, however, the spread and strength of these operational norms will depend on education of consumers and market mechanisms: perceptions of better quality, on one hand, and suspicions of possibly compromised ICT, on the other, can drive the growth of a market segment for secure hardware and assured software. The development of such norms is something of a necessity for most states. The alternative is for states to have components for military and critical infrastructure systems manufactured under their direct control, as the United States now does and China and Germany are planning to do. But that would be too costly for many states and providing the needed, trusted oversight could be beyond their capabilities.

Like minded-states that have agreed to collective cyber defense will need to satisfy certain technological needs to support norms of information sharing, assistance in disaster and attack, cooperation in forensics, and collaboration in analysis of attacks. These needs will include shared data formats, repositories, structured queries and analytic methods. As these norms and technologies suggest, collective cyber defense will involve states and organizations in the collection of even more copious information, especially for the provenance of components and packets. Such expectations raise questions about the future of anonymity in cyberspace. It should be noted that the present situation is not good with respect to anonymity. Current networks do not guarantee it, but they also fail to provide adequate provenance for cybersecurity. Providing provenance everywhere would enable cryptographic strength attribution of sources, but at first blush it would it would weaken anonymity. That could chill the flow of information and threaten the freedom of legitimate – non-malign -- sources, such as organizers of protest movements in authoritarian countries. (Data for anonymizing networks shows that use drops immediately after upgrades to packet inspection and filtering by state authorities; use picks up again with the introduction of new circumvention techniques.) Nevertheless, according to some participants the trade off between anonymity and provenance tracking was not inevitable and some emerging technologies may have the potential for realizing both.

Finally, some workshop participants suggested that the technological norms and best practices for enhancing cybersecurity should reduce the human footprint in cyber systems, since organizational hygiene and other human oriented security policies had their limits. Indeed some currently implemented practices, like automatic patch updating, ISP-level scanning for malicious email, sanitization proxies, are aimed at automating hygiene by getting people out of the loop.

Public-Private Partnerships: The UN resolution for cybersecurity, various national strategy papers and even the Russian draft convention for international information security expect the private sector to play a significant role in protecting cyberspace. Consequently, there should be support for a campaign to encourage states to develop organizational frameworks or at least working relations with local and international private companies to accommodate this participation. The acceptance at the operational level of such a norm can create a “win-win” situation: The companies frequently have more capabilities and practice in dealing with threats in cyberspace, but often need authorization from states to act more effectively, as demonstrated by the collaborations against Conficker and other recent malware pandemics.

These collaborations of ISPs, vendor, some governments and researchers reveal the presence of several “invisible norms,” or regular practices, based on the willingness of system operators to cooperate in keeping their networks clean. Because of Conficker’s extent, the collaboration grew to over one hundred top level domain operators and Microsoft, in daily touch with ICANN and less frequently with governments. These partners implemented an extensive strategy of prevention, through blocking botnet command and control sites, and remediation, through the disinfection of host computers. This collaboration exposed the difficulties of cooperation at the legal / policy level compared with the relative ease of cooperation at technical levels. In some countries, there was a need to work around legal hurdles, for instance, contractual barriers to take down, anti-trust laws, protection of privacy. Major legal difficulties were avoided, because the prevention strategy could be implemented locally, through blocking at the name (for the C&C) resolution level, and did not require any transborder activity. But despite their success, anti-Conficker Cabal and other anti-malware collaborations had an *ad hoc* character, with ICANN and other stakeholders lacking the authority to institutionalize the mechanism.

The organization form for the public-private partnerships will vary over states. In some European countries, these partnerships are well developed for many sectors and domestic laws to support them are in place. In other countries ICT trade groups exist for information sharing, but governments have sometimes lagged in connecting to them. In less developed countries, there are few such partnerships. National and international organizations, with experience in public and private sector partnering on economic matters, e.g., the Asian-Pacific Economic Cooperation (APEC), should be encouraged to guide and nurture the growth of partnerships in such places. However governments and companies might have different visions and desire different tempos in implementing their partnerships. For example, companies like Goldman Sachs or Lockheed Martin, which operate globally will want to harmonize the rules across countries, while a government, even if it views itself as an enabler, will face local and legacy issues that might keep it from accepting such norms. Also some companies might anticipate that by meeting the standards set in their cybersecurity partnership, they can deflect regulation by the government partner in the future. A government agency that suspects such a motive might then move cautiously in such a partnership. In view of these possibilities, perhaps the most states can expect of one another – and what can be formulated in a norm -- is they will seek partnerships with the private sector to assure a clean and healthy Internet.

The discussion of these partnerships also voiced concern that ISPs' inspection and remediation activities can approach unauthorized surveillance of their clients, e.g., spam filtering, collection of use data for commercial or political use. This can be particularly ominous in countries lacking commitment to the "rule of law" or civil rights. Consequently the encouragement of such partnerships should be include a norm of transparency and limits in private companies' surveillance and data collection policies.

Internet Freedom and a Global Information Society: As noted earlier, Internet Freedom or the free, unfettered flow of information, has been a very contentious issue with regard to both daily operations of the Internet and governments' positions on the Internet's administration and future. This is both a human rights and a cyberspace issue, since the rights to information, expression and association have underpinned the use and growth of cyberspace. Yet that growth itself has led to push-backs from states whose political and cultural traditions are quite different from that of the liberal democracies where cyberspace first developed. While paying lip-service to the human rights, these states have claimed that national security concerns, such as internal social stability and terrorist threats, require some restrictions on these rights. In some cases these claims are self-serving and protect authoritarian regimes. In others, they can be partly justified by evidence of ethnic violence or insurgency. In any case, in response to the cyber fueled upheavals in the Middle East, states have increased their restrictions on Internet and social media use. More than forty countries now involved in developing second and third generation filtering techniques. At the international policy level, many of these same states are trying to create a norm of the state as the final arbitrator of the Internet within its territory, through promotion of the ITU as the appropriate agency for Internet governance, and with the disparaging of ICANN and the associated multi-stakeholder model.

In response, the United States and the like-minded, western democracies continue to champion the idea of cyberspace as a domain that should be free of political interference and where freedom of expression and to information are guaranteed. This position considers those freedoms as human rights in themselves and indispensable for development and innovation in cyberspace. However the institutional arrangements which it claims are needed to protect these freedom are more contingent. ICANN and the IETF have served the independence and development of the Internet fairly well, but their usefulness may be coming to an end. They do not have a compelling narrative to mobilize organizations for the defense and development of cyberspace nor enough institutional strength of their own to counter the state-centric models proposed by Russia, China and other nations. According to critics they have not speedily or sufficiently accommodated the demands arising from the shift in Internet demographics and from the tremendous growth of mobile computing, social media and clouds. Moreover, Chinese cyber experiences suggest that the choices might not be as binary and stark as the U.S. portrays them to be: Despite the authorities' massive efforts to control Chinese information space and suppress undesired political speech, they have not created a Gulag, but rather a cat and mouse game with politically involved citizens. They have chilled but not stilled political conversations. And notwithstanding this repression, cyber media have thrived there and greatly benefitted China economically and socially.

Regardless of the strength of its argument, the United States' high-profile embrace of a norm for Internet Freedom is a good tactic, because it forces international conversations about the Internet to a focus of this issue as much as on governance. It may also provide one avenue for co-opting the ITU or, at least, diminishing the Chinese influence on it, since the ITU formally recognizes access to information as a universal human right. However, an absolutist position on such freedom, will not succeed, because boundaries on that freedom are already being set and contested even in "like- minded" countries, in the name of national security, intellectual property rights, commercial enterprise, social harmony, etc. So policy makers who support the norm may have to allow considerable latitude in its interpretation and applicability.

4. Conclusions

Development and adoption of norms: Governments are ready to discuss international norms for cyberspace because they are increasingly insecure and often aggrieved by some state and non-state actors' behaviors there. Getting states to agree on some mutually acceptable norms is like getting them to take pledges of good behavior. It might not have lasting effects, but, for the time being, it stabilizes their expectations of one another and suggests recourse, if these expectations are not met. In this sense the articulation and acceptance of norms at the international level provide means for states to avoid, recognize and manage conflict.

Another reason why states should be and are considering cyber norms is the recognition (mostly implied) assumptions that underpinned the Internet, including those for the relative neglect of security, may no longer hold. Often norms articulate or reflect accumulated experiences, best practices, lessons learned, contracts and principles. Even norms for socially appropriate behavior often imply a convergence toward the mean of the distribution seen, as if our desires are tempered by our knowledge of how people really act. However, the development of the Internet has been so dynamic and multifaceted, that the distributions are not normal. Without some recognition of new realities, e.g., the demographic changes in user population, and the abandonment of some old expectations, it will be difficult for states and other stakeholders to strengthen or build institutions that support a clean, healthy, trusted cyberspace.

Norms have life cycles. They are proposed, articulated, advocated, contested, accepted, modified, turned into standard operating practices, often made into laws, transcended and abandoned. Frequently, norms for new situations and areas of human interaction are extensions of old norms. Recent studies of international norms have observed that shocks, norm entrepreneurs and personnel are necessary for bringing about change in the prevailing norms. The shock gives people reason for change, the entrepreneurs articulate possible changes, and the personnel evangelize and implement them. The US and NATO received their shock for cybersecurity from the DDoS attacks on Estonia in 2007. During subsequent debates over the feasibility of cyber deterrence, the need for a cyber command and other issues, would-be entrepreneurs articulated new norms, including new organizational models. While US allies have not followed the US lead in setting up a cyber command, they have implemented organizational changes to better coordinate cyber defense, and NATO has adopted new policies and procedures to the same end at a regional level. The US and its allies US are now training personnel for implementing the new policies and norms.

The Chinese-engineered security breaches at Google and Google's decision in turn to flout China's censorship law, were shocks that brought Secretary of State Clinton to a norm entrepreneurial moment – the high profile, public embrace of Internet Freedom. Her statement in January, 2010, perhaps expressed a more intense commitment to an existing norm and policy on its behalf, than articulated a new one: the State Department was by then funding facilities and training in evading Internet filtering. Similarly, recent proposals by China and Russia on information can be read as responses to the shocking, social-media powered, regime-toppling Arab Spring, 2011, but they are also consistent with these countries' proposals last decade. These proposals themselves responded to dissidents' and separatists' use of the Internet for propaganda and recruitment, but they also extended traditional media control norms to new media. In short, these and other potential cyber norms have gone through various stages of their life cycles. These processes might tell us something about the possibilities for effective, widely accepted norms in cyberspace.

Respective proposals by the US, Russia, China and the IBSA countries on Internet governance, cyber conflict management and information rights/ control present a grand debate on what the Internet (and more generally cyberspace) should look like: a Westphalia/ UN Charter system or the slightly modified current one, underpinned by the founding assumptions and existing norms? To the extent that proposed norms are anchored in such visions, they will be contested and fail to gain widespread support. A strategy of disjointed incrementalism would therefore seem more likely to succeed in promoting any particular norm. The United States government appears to have recognized this in advocating for particular norms at different international forums. It has continued traditional negotiations over standards at the ITU, At the United Nations, it has called upon nations to develop their own cultures of cyber security and preparedness. Following its policy shift toward readiness to discuss cyber norms for international security, it has tried to root such discussions in existing, globally acceptable Laws of Armed Conflict (LOAC) and their extension to cyber conflict. It has also placed on the agenda discussion of norms regarding proxies, e.g., criminal organizations, for state purposes.

A workshop participant noted that the potential of disaggregation to win widespread support for a proposed norm is shown in how the UN came to agreement on countering the use of the Internet for terrorist purposes. The working group of the Counter-Terrorism Implementation Task Force (CTITF) that developed the adopted proposal found that an overall convention was not needed and efforts for one would be counterproductive, especially in the absence of a common language or UN convention defining terrorism. Instead, issues could be compartmentalized and moved forward individually. A strategic framework, which defined the dimensions of an issue and the obstacles facing it, was then used to identify easy wins, i.e., areas of agreement. These wins were effective in building confidence in the process and trust among UN members that the agreement could make a difference in cyberspace.

Another participant commented that an effort in public diplomacy (Track 2) between Russian and US non-governmental teams likewise showed the benefit of disaggregating issues for norm development, as well as the difficulties in finding a common language. These teams sought to develop a common vocabulary for cyber incidents, as a basis for mutual understanding and trust. Through lengthy discussions and on the basis of logic, the Americans convinced their Russian colleagues to distinguish between attacks and exploits of hosts, operating systems and networks, on one hand, and threats created by the content of information. This break through could portend wider acceptance of cyber security norms, in the US sense, but its sequel also highlights a point made more generally by another participant: at every stage, norm development can be derailed by particular interests: The Russian Foreign Ministry, upon learning of the result, called upon Russian team to drop the distinction it had made.

In contrast, the fight against Conficker, reported earlier, and the collaborations among national CERT's, especially among Japan, Korea and China CERT's, indicate that international cyber norms develop more rapidly and widely the more closely they structure or reflect expectations in frequent, international interactions, to stabilize technical operations. Generally, network operators expect cooperation from one another on the basis of their interdependence – the idea that "your security is based on ours," and vice versa. Among the Japan, China and Korea CERT's this expectation is deepened through frequent trilateral conversations, and an implied duty to respond to calls for information or assistance, with failure to respond taken as a signal. Transparency in response to incidence and de-escalation mechanisms for potential conflicts are efficacious and confidence building viz., a CERT can ask its relevant government minister to intervene through his/ her opposite number in the attack's presumed country of origin. These CERT's also expect one another to take clean-up actions in their respective domains, following an incident; they also subscribe to a higher level, if vague, norm of a "clean Internet." This alliance and its norms are gaining influence; its personnel have briefed and trained personnel from other CERT's and regional alliances of CERT's. The members of the alliance derive power from their being national CERT's, but this status might also constrain their freedom, since a CERT's government sponsorship could be withdrawn in case of a conflict over policies. So while, their model can be replicated globally, that would have limited effect in shaping cyber norms at the global level.

Priorities: The establishment of norms of behavior for international cyberspace quintessentially fits what international relations theorist Arnold Wolfers called a "milieu goal". By that he meant situations, patterns or regularities whose attainment would enable a state to maintain its position in an international system or more easily obtain more tangible assets, which Wolfers called "possession goals."[19] Because states are interconnected and interdependent in cyberspace, on one hand, and threat capabilities have proliferated rapidly, on the other, an optimal milieu

[19] A. Wolfers, *Discord and collaboration: essays on international relations*. Baltimore, MD: 1962, cited in J. Nye, *The Future of Power*. New York: 2011, 16.

pertains when all states accept the same norms and these tend to conflict avoidance and non-interference. For that reason, state officials who believe that the acceptance of norms by states can help secure their state's cyber activities should promote only a small number whose acceptability has already been signaled by key actors. The review of candidate norms identified five meeting these criteria.

- States should distinguish between disruptive and damaging cyber attacks and evaluate a damaging attack on the basis of its scope, duration and lethality;
- States have a duty to assist other states that have suffer a major cyber attack or disaster, and also have a duty to inform others of new threats in cyberspace;
- States should cooperate in the certification of ICT supply chains;
- States whose territories or citizens are involved in transborder cyber activities which are unambiguously criminal in their states should cooperate in the investigation of these crimes and the apprehension of their perpetrators;
- States should enable the formation of public-private partnerships for cybersecurity, which include both local and international ICT companies operating in their territories.

These potential norms can win widespread support for two reasons. First, with the exception of cooperation in criminal investigations, they are directed toward reducing vulnerability and confrontation rather than in suppressing threat actors. In some sense then, they demand less action from the state actor, but if all states behave according to these norms, there will be significant reduction in threats and conflicts. Second, these norms are more concerned with maintaining cyberspace for all states rather than satisfying particular parties' agendas. Put another way, they are *status quo* oriented. They respond to that vision of the Internet as a network whose value grows with the number of its users and thus to a expanding positive sum or classic cooperative game. There is, of course, a concurrent competitive game being played between states over this same game board, with rewards, such as status and power, that lie beyond it. For that reason, cybersecurity strategies need the additional components of technological transformation and "reasonable deterrence."