A Preliminary Report on the Cyber Norms Workshop

Roger Hurwitz, co-chair[1]
with Camino Kavanagh, Tim Maurer and Michael Sechrist, rapporteurs

The following are the co-chair's reflections on the discussions and findings of the cyber norms workshop, conducted at MIT, Oct. 19-21.[2] The workshop's purpose was to depict the needs and benefits of norms for various cybered behaviors and to propose norms whose cultivation could reduce insecurity, instability and misperceptions at international levels in cyberspace. The workshop participants included 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. The workshop sessions were highly interactive, but had no formal consensus seeking or recommendations selection. Therefore, when terms like "the participants agreed" appear in this report, they express only the writer's sense of the participants' views. He bears sole responsibility for such attributions.[3]

The role of norms in regulating international behaviors, with relevance for cyber:

Norms are shared expectations about appropriate behavior. They may either be descriptive of current practices, or prescriptive, that is, specify the 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, a state's acceptance of a norm puts its reputation at risk. So when a state 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.

The current willingness of states to discuss international norms for cyber behaviors respond to their leaderships' and publics' growing sense of insecurity and threats in cyberspace. The threats include cybercrime, cyber attacks on critical infrastructure (DDoS, Stuxnet-type malware), political and industrial espionage, cyber-enabled terrorism, cyber-enabled regime threatening protests (e.g., the Arab spring), widespread restrictions (censorship, filtering) of Internet use, and the proliferation of the means to achieve all these. Some threats also jeopardize the roles the Internet and other cyber applications play in economic and social development. Consequently, states

[1] Contact address: 32-263, CSAIL, MIT, Cambridge, MA 02139, USA. rhhu@csail.mit.edu

[2] The workshop was sponsored by the Canada Center for Global Security Studies at the University of Toronto, the Belfer Center for Science and International Affairs at Harvard Kennedy School of Government, Explorations in International Cyber Relations, a project at MIT and Harvard, Microsoft Corporation, and MIT's Computer Science and Artificial Intelligence Laboratory (CSAIL).

[3] The workshop was conducted under the Chatham House rule. Accordingly no participants are named in this report, so no remark can be attributed to any of them. However, a list of participants is appended to the report.

have begun to perceive they have a common interest in limiting their creation of such threats and in cooperating to suppress them. Ways of pursuing these interests might be specified in cyber norms.

The workshop participants had a more proactive outlook. Many agreed that **the goal of cyber norms should be 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 [to assure] "a trusted and secure global environment to sustain (peaceful) commerce, communications, international peace and security."

While cyberspace is a relatively new medium[4] for international activities, the identification and cultivation of norms for it do not start *ab nihilo*. Rather they can build on a considerable body of custom, laws and practices pertaining to international spaces, e.g., air, sea, and activities within them, e.g., war, trade, which can be selectively extended to cyberspace. So the focus in discussing cyber norms need not be on creating new ones, but in interpreting existing international norms for cyberspace, and determining their limitations. Consequently, the development of cyber norms or giving existing norms cyber specific content will depend on practice in which such limitations and novel needs are discovered. These discoveries could conceivably enable policy makers over the course of international meetings to construct a framework for cyber norms – a step that would enhance the consistency of the norms across the various behaviors and situations they would address.[5]

However, a generally accepted, comprehensive set of norms might be too ambitious a goal. States today differ in their visions of cyberspace, especially with regard to issues of information access, sovereign authority and responsibilities. Also, they do not similarly rank the threats. Consequently, general agreements on where to begin might be limited and the specification of norms might be slow and piecemeal in coming. 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 took note that **different cyber norms might apply to a state's relations with other states at the bilateral, multilateral – say, within a group of allies – and the global levels.** For example, a signatory to the Budapest Convention might share information for computer forensics only with other signatories. Similarly, China's reasonable expectations would be that only other SCO members will suppress dissidents' information flows from servers in their territories. Still, some participants noted that it is common for states to observe an international norm without formally accepting it, as seems the case for most provisions of the Budapest Convention. In other words, the articulation of a cyber norm can be effective in changing

[4] Whether to characterize cyberspace as a commons, condominium, domain, eco-system or socio-technological system has caused some controversy, since cyberspace partakes of some but not all of the attributes for each, and each term has some added significance for one or another stakeholder type.

[5] This vision raises questions about the appropriate fora and levels of representation for such meetings, and more generally about governance institutions for cyberspace, but their answers are beyond the scope of these remarks.

behaviors, even in the absence of general acceptance of the norm and a coalition of the "right-minded."

The workshop participants also noted the multiple dimensions of international cyber activities and the various contexts where cyber norms could function, including war, domestic security, economic, political and social interactions. Some agreed that the **crafting of norms for these should be guided by the following key principles**:

1. Cyberspace should remain open, interoperable and reliable;
2. 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;
3. All nations have an interest in a cyberspace that retains the trust of its users;
4. Fundamental freedoms of people for information and connectivity need by upheld;
5. Key international laws, norms, and rules should be extended to cyberspace;
6. Multi-stakeholder stewardship, involving governments, international organizations and the private sector, should shape the development and maintenance of the Internet;
7. Governments should refrain from political interference in technical development and standards for the Internet.

Norms regarding military operations in cyberspace

In principle the Laws of Armed Conflict (LOAC) should be applied to such military responses and operations. In practice, there is insufficient experience with the use of cyber in war and war-like contexts and insufficient knowledge of adversaries' capabilities for a blanket extension of LOAC and non-problematic rules of engagement. Quite possibly cyberspace does not afford making the clear distinctions of military/civilian, attack/ espionage, intentional/accidental, state/non-state, which enable LOAC to operate in the kinetic world. The restraint, which states have apparently shown in the use of cyber weapons, might thus be due more to fear of retaliation or unforeseeable consequences, than to any normative constraint. Furthermore, LOAC as effective constraints and enablers on military activities depends on deep intuitions and daily practices of military personnel, but the socialization in the use of cyber stems from a technology world, that originally did not anticipate malicious behavior and only lately has begun systematically dealing with it. Finally, political leadership in most states has shied from specifying the level of cyber attacks that would consider tantamount to armed attack and trigger a right of self-defense. This reluctance is evident, for example, in NATO's acknowledgement that some attacks might invoke Article 5, but it would depend on political leadership to decide whether the current attack rises to that level. In view of these ambiguities, some workshop participants agreed on **the desirability of confidence building measures, e.g., a cyber hotline, greater differentiation of cyber incidents, and finding mechanisms for crisis management and de-escalation.**

Workshop participants also noted the development of **a structural norm (practice) of military involvement in the protection of domestic critical infrastructure from cyber attack.** This norm, enabled by national policies, legislations and structures, will thicken a state's cyber defense, can enable it to draw on the resources of its military allies when its cyber-dependent critical infrastructure is under attack and may lead these allies to harmonize their cyber-related laws. However, like terrorism, **the norm/ practice also raises the question of applicable rules-of-engagement, when the attackers are non-state actors.**

Norms regarding political, military and industrial espionage

The use of cyber technology for espionage has challenged the viability of traditional norms regarding espionage – not a violation of international law (and justification for war), but prosecuted under domestic law. Specifically,

a) cyber weapons can steal, on an unprecedented scale, political and military secrets and intellectual property;

b) the weaponization of cyber systems used in intelligence, surveillance and reconnaissance blurs the line between espionage and attack. For example, Stuxnet can be characterized as an engineered threat, intended to damage critical apparatus through hijacking controls, rather than an exploit that takes advantage of vulnerabilities, created as a by-product of cyberspace's generativity. This goes well beyond the interruption of an information system, which the UN Charter does not consider armed attack.

Large scale political and military espionage occasionally occurred in the pre-cyber age, and, when discovered, could draw a sharp response from the victimized country, a departure from its usual policy of toleration, e.g., the UK's 1971, expulsion of over 100 Soviet spies working under diplomatic cover. Today, 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.

The US and most of its allies believe that industrial espionage by state actors should not be condoned by international law, since it cannot be justified as a response, to a national security concern, e.g., intelligence gathering, or part of anticipatory self-defense. The US expects the norm of no industrial spying to be observed among its allies, but has been less forceful in demanding it globally or in its bilateral relationship with China, the principal source of such espionage. The workshop took note of a **proposal for a norm that bans large scale commercial espionage, which the US and like-minded nations could promote as a universal customary norm to multiple international bodies and incorporate in its bilateral relations**, much as it did the proliferation security initiative (PSI). For the US and probably other countries, giving this norm "teeth" would need changes in laws, so that foreign nationals could be prosecuted for economic espionage originating outside national boundaries. Acceptance of the norm by a respectable number of states would provide a basis for "officially" charging a persistent violator and creating a series of sanctions, perhaps determined at the World Trade Organization. Obstacles to cultivating such a norm, however, are the difficulties in changing domestic laws, problems of assessing the extent of damages and providing evidence for the charges both in domestic courts and international forums. The US intelligence community is unlikely to engage in damage assessment or provide the evidence, because its involvement could damage any criminal investigations, while also jeopardizing its sources. Such a norm may also ban some activities of the intelligence agencies themselves.

Several participants also noted the growing trade in cyber espionage and surveillance services by security and defense contractors in developed countries to authoritarian regimes for use against political dissidents. The sense of the workshop was **such commercial espionage violates the norms of information freedom and**

that governments of the developed countries should consider regulation of this trade.

Norms regarding cybercrime

International norms and coordinated practices to address cyber crime are essential, because the cyber criminals are more important as a threat to a secure cyberspace than any one of their crimes, costly as they might be. The cybercrime organizations breed new attack techniques, and their capabilities, when augmented with outsourced specialized skills, exceed the capabilities of all but a few states. Their willingness to sell these capabilities, however, decreases the interest for many states in norms targeting cyber crime and criminals. Although the US itself follows **a norm of not hiring criminal hackers**, the norm is not easily exported, since many states would like to have the criminals' capabilities available. Their view, which echoes practices of security agencies using criminal informants and operators, is a problem, which discussions of cybercrime might diminish by noting that some cybercriminals can become existential threats to the state – blowback on steroids. In other words, a **norm that states (other stakeholders) educate themselves about cybercrime** is a key component in developing effective norms in this area**.**

The formulation of subsequent norms will need to recognize

- the technological obsolescence of practices for cybercrime prevention;
- the weakness of existing agreements for cooperation in investigations;
- the problems of different jurisdictions in transnational crime,
- difficulties in securing the cooperation of relevant publics and stakeholders,
- the possibility that police work is structurally unable to reduce cybercrime.

In the decade since the Budapest convention, Internet use, mobile devices, including implanted medical devices, and collection of data have all grown exponentially, increasing by magnitudes opportunities for cybercrime and even creating new crime categories, such as rape of an avatar. Yet security policies at the organizational level have not kept pace. For example, the removal of data silos within the US military was not accompanied by restrictions on the amount of information a user could download – a lapse that allowed Bradley Manning to download the Wikileaks cables. While the USG has belatedly introduced preventive measures, it has not discussed such measures with other states to reduce similar risks to them and its own interests. Such opportunities and risks will multiply as data moves to the cloud, but new, secure interoperability standards lag. The panelists at the workshop session on cybercrime agreed that these changes demand, at the very least, a **norm for the USG and its allies that their computers be encryption enabled and all data placed in the cloud be encrypted**.

The Budapest convention provides an inadequate basis for international cooperation to address cybercrime. It did not distinguish among cyber crimes, specified no requirements for data retention across signatories; it did not discuss cross-border law enforcement procedures and transporter for searches and seizures. Moreover, during the negotiations no major effort was made to convince Russia or China that cooperation for crime enforcement is in their interests. Such an argument might now be made to China in conjunction with a **norm distinguishing between low and high criminals and expecting cooperation in the pursuit of high criminals**. Such a norm would require data retention and accessibility for certain types of crime. Clearly that would demand states compromise some sovereignty, but the advent of the cloud will in any case force states to some compromises regarding their jurisdiction on control and handling of data. More focused targeting on the criminal conducts of common interest can promote the acceptance and implementation of this norm, by reducing the demands for cooperation. For example, technology enabled studies can identify the constraints and choke points, e.g., means of monetizing, for various cybercrimes, so prevention – a "draining of the swamps" – and investigation can be more effective and routinized, while consuming fewer resources. However, we should not expect a norm of cooperation in criminal prevention and investigation to go global, no matter how little it demands of adhering states, because many developing countries lack the capacity to cooperate, while some governments or their officials will want to (continue to) enjoy the benefits of giving cybercriminals safe harbor.

Given the technological and legal challenges facing police in preventing and investigating cybercrime, discussion at the workshop turned to possible roles for other stakeholders and the public, implied by proposed **norms of a duty to warn (or inform) and a duty to assist**. The duty to warn or inform becomes increasingly relevant with the growth of situations where individuals, organizations or governments are unaware their information systems are at risk or their data has been stolen. It has already been formalized in many jurisdictions' mandatory notification laws and institutionalized at the international level in data sharing procedures among CERTs and NATO allies. To some degree, warnings of risks and loss will also be expected from cloud vendors. However, some entities have rebuffed or avoided this expectation due to its imposition of processing costs, reputational risks and disclosures of possible improprieties in data collection. They may reject the legislation of this duty on the more principled grounds that it permits governments to intrude in the conduct of their business and even override their contractual obligations. Also, the norm will be unevenly practiced at the global level – eschewed in particular by governments, which own or tightly control ISPs in their territories.

The duty to assist in response to a E-SOS and according to the victim's choice is an extension to cyberspace of maritime practice. The norm could be cultivated at various levels and would create expectations of action by individuals and organizations, as well as governments. Originally conceived with a background model of DDoS attacks, as in Estonia, 2007, the extension of this proposed norm for assistance and remediation of cybercrimes reflects the limits of police in coping with cyber crime and the consequent devolvement of responsibilities to private individuals and organizations. This is not necessarily a surrender, because a global company, like Microsoft, which operates in 200 countries, can marshal more resources and expertise to constrain transnational cybercrime than can a national police force, like the FBI, which has only 70 offices outside the US. Indeed, Microsoft has had some success with a novel legal strategy that seeks in a variety of jurisdiction to close down botnet C&Cs.

One extension of the duty to assist, which provoked discussion, is the letter of marque, in this case state commissions for an individual or organization to attack/ disrupt networks used in cyber crime. One participant likened this to the use of bounty hunters by criminal justice system, while others noted that some private companies are already engaged in such activities directed at hackers affecting their own operations. However, **a norm encouraging letters of marque,** regardless of how limited the commission, would indirectly sanction proxies, and the escalatory effects might therefore well outweigh any direct reductions in cybercrime.

Norms for Technological Foundations for Secure Cyberspace

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. On the industry and research community's views, states' appropriate roles in promoting such a change, as well as defending the existing Internet, are captured in the following norms:

- **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, 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. Such action, however, is worthwhile, since good ICT standards by reducing opportunities for bad cyber behavior, can contribute to international stability.

The panelists at this workshop session also noted measures and roles, which when adopted by various players, consistent with a multi-stakeholder model of responsibility, would enhance cyber security and defense. Specifically,

- academia should develop shared, open source reference standard to assure network components and develop processes for verification and rapid accreditation of the produced components produces;

- Global standard for strength and circumstances for encryption need to be developed;
- Identity management needs to be handled in terms of international digital identities, authentication standards and their legal status;
- Governments, especially the USG, should through their purchasing and legislative power help create market mechanisms and incentives for ICT products, including hardware, software, networking and communications equipment, cryptography and authorization management;
- Governments must also desist in supporting/ allowing black markets for cyber crime and vendor installations of trojans in commercial ICT products.

Like these norms and practices to be cultivated at the global level, **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. **The needed norms 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**. Governments would need to agree – arguably Russia and China have as much as the US and other developed countries have an interest in trustworthy cyber components. Large global companies, on the both the supply and consumer sides, would need incentives to enter such a system. Ultimately, however, **the spread and strength of these norms depend on market mechanisms:** perceptions of better quality and eventual cost benefits can drive the growth of a market segment, in this case, one for secure hardware and assured software.

While global norms for collective cyber defense might prove elusive because of differences across states in the definition of cyber attack, **like-minded states can improve their collective cyber defense on the basis of norms that routinize information sharing, assistance in disaster or attack, cooperation in forensics, and collaboration in analysis of attacks.** Keys to the needed coordination are developments of shared data formats, repositories, structured queries and analytic methods.

Note these potential norms expect states and organizations to collect copious information, especially for the provenance of components and packets, and such expectations raise questions about the future of anonymity in cyberspace. Current networks do not guarantee anonymity nor provide adequate provenance. Providing provenance everywhere would enable cryptographic strength attribution of sources, but by weakening anonymity, it could reduce the free flow of information and threaten the freedom of legitimate sources, such as organizers of democratic movements. (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 work-arounds for the new capabilities.) Nevertheless, anonymity and provenance are not necessarily tradeoffs. According to the session panelists there was potential for achieving both through revocable cryptography or another emerging technology.

Some workshop participants suggested that the technological efforts to improve cybersecurity should include efforts to reduce the human footprint in the systems, since organizational hygiene and other human oriented security policies had their limits – though the obvious analogy to automobile safety was not mentioned. Indeed some current efforts, like automatic patch updating, ISP-level scanning for malicious email, sanitization proxies, are aimed at automating hygiene by getting people out of the loop.

Normative bases for public-private partnerships/ defensive coordination

The collaboration of ISPs, vendor, some governments and researchers in fighting recent malware pandemics, most notably Conficker, indicates the presence of several "invisible norms," i.e., structured 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, legal hurdles, e.g., contractual barriers to take down, anti-trust laws, had to be overcome. Greater 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 have had an *ad hoc* character. ICANN and other stakeholders lacked the authority to institutionalize the mechanism.

Yet even this ephemeral collaboration raises the concern 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. On a democratic view, **a norm for public-private partnerships would need to limit or call for arrangements that limit (or specify circumstances for) private companies' surveillance and data collection**.

Common concerns and a nominal willingness to cooperate do not, of course, guarantee the development of an effective public-private partnership, especially in the absence of an emergency. One session panelist, who worked on partnering governments with underwater cable operators, noted that simplicity is a best friend for building such partnerships. In his experience, some confidence building measures, like mutual recognition of the common concerns, are a needed first step, on whose basis the potential partners will be more ready to listen to one another and overcome hostilities based on narrow self-interest. Other panelists pointed out that **national and international organizations, with experience in public and private sector partnering on economic matters, would be the most congenial for growing such partnerships for cybersecurity**, with the Asian-Pacific Economic Cooperation (APEC) a leading example. Even so, the governments and companies might have different rates at which they want or are able to set up rules and practices for their partnerships. For example, companies like Goldman Sachs or Lockheed Martin, which operate globally will want norms that apply worldwide, 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 satisfying a norm or standard set by their cybersecurity partnership, they can deflect regulation by the government partner in the future. A government agency that suspects this is the private sector's motive might then move cautiously in such a partnership.

From the technical perspective, public-private partnerships are vital means for cyber security and defense, because the private sector can offer needed skills and resources. However some governments will not want to share their regulatory power with the private sector. On the other hand, some companies would refrain from joining in the belief their participation would not have a reasonable "return on investment." Indeed, given the current organizational structure of cyberspace, it is not clear how much ROI such partnerships can deliver. As noted earlier, ICANN failed to established a DNS CERT and could not institutionalize the type of public-private collaboration that dealt with Conficker. **So the appropriate norm might then declare "that governments should seek cooperation with the private sector to assure a clean and healthy Internet,** but not specify the organizational form this cooperation should take.

Norms for Internet Freedom and a Global Information Society

Freedom of expression and, with the advent of social media, freedom of association have underpinned the use and expansion of the Internet. Some regimes have feared these freedoms, however, and their number has grown with the expansion of the Internet. In the past several years, state activity and geopolitical contestation over the Internet have increased dramatically, with 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 or eco-system that is free of political interference and where freedom of expression and access to information is guaranteed. Their position might be critiqued on the grounds that they have neither forged a strategic narrative, in which defense and development of the Internet are assured, nor proposed an architectural framework to counter the models proposed by Russia, China and other nations. The architecture and institutions to which they cling have fostered technological development as well as democratic ideals, but they are now at the end of their life cycle. These do not sufficiently accommodate the shift in Internet demographics to the East and South; they do not give newbie states seats at the decision making table; they are not accommodating the great, ongoing growth wave in mobile computing and in the cloud.

Finally, the critics question whether the demand for openness and free flows of information are motivated and defined more by the interests of American hardware and software vendors, then by a concern for democratic values and development of Internet users. Arguably, the securitization of cyberspace, manifested in the standup of cyber commands, might also chill the flows of information. In depicting cyberspace as wild and threatening, the securitization narrative overstates the cases and ignores the positive contributions of the Internet to economic and social development, even where filtering is practiced. As one workshop participant commented, the filtering in countries like China does not create a Gulag, but a cat-and-mouse game between governments and their politically involved netizens.

Nevertheless, the United States did take a significant in its high-profile embrace of a norm for Internet Freedom, even if that norm fits rather awkwardly with securitization in the US cyber policy bundle. As a tactic, this introduction of Internet Freedom as a core value in international conversations about the Internet forces those conversations to a focus of the US's choosing. It may also provide one avenue for co-opting the ITU, since that organization formally recognizes access to information as a universal human right. At the strategic level, advocating Internet Freedom is doing the right thing. However, when the boundaries of that freedom are being contested even in "like-minded" countries, to say nothing of the embarrassment of Wikileaks, absolutism is untenable. So some modification in the proposed norm can be expected that allows for **ambiguity and reduces friction regarding the standards of Internet Freedom**.

Reflections on the life cycle for cyber 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 CERTs, especially among Japan, Korea and China CERTs, 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 CERTs this expectation is deepened through frequent tri-lateral 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 CERTS 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 CERTs and regional alliances of CERTs. The members of the alliance derive power from their being national CERTs, 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.

10/30/11

Cyber Norms Workshop Participants

Suleyman Anil, Head, Cyber Threat Division, NATO

Charles Barry, Senior Research Fellow, Center for Technology & National Security Policy, National Defense University, Washington, DC

Joel Brenner, Cooley, LLP, former National Executive for United States Counter Intelligence

Steven Chabinsky, Deputy Assistant Director, Cyber Dvision, Federal Bureau of Investigation, (US) Dept. of Justice

Nazli Choucri, Professor, Political Science Dept., MIT

Paul Cornish, Professor of International Security, University of Bath

Andrew Cushman Senior Director, Trustworthy Computing, Microsoft Corporation

Ronald Deibert, Professor & Director, Citizen Lab/ Canada Centre for Global Security Studies, University of Toronto

Chris Demchak, Professor, Strategic Research Dept, Center for Cyber Conflict Studies, US Naval War College

Greg Dempsey, Senior Policy Officer, Foreign Affairs and International Trade, Canada

Martha Finnemore, Professor, Political Science Dept., George Washington University, Washington, DC

Jack Goldsmith, Professor, Harvard Law School, Harvard University

Mark Goodman, Cyber Crime Research Institute and Singularity Univesity

Amy Gordon, Director, International Peace and Security Program, The John D. and Catherine T. MacArthur Foundation

Melissa Hathaway, President, Hathaway LLC & Senior Advisor, Harvard Kennedy School of Government, Harvard University

Duncan Hollis, Professor and Associate Dean. Temple University School of Law, Philadelphia, Pennsylvania

Rex Hughes, Rex Hughes, Assistant Director, Cyber Defence Project (CDP) at the Cambridge Centre for Science and Policy (CSaP), Cambridge University

Roger Hurwitz, Research Scientist, Computer Science & Artificial Intelligence Laboratory, MIT, and Senior Fellow, Canada Centre, U. of Toronto

Nigel Inkster, Director of Transnational Threats and Political Risk at the International Institute for Strategic Studies, London

Yurie Ito, Director for Global Coordination, Japan Computer Emergency Response/ Coordination Center (JPCERT/CC)

Sean Kanuck, National Intelligence Officer for Cyber, National Intelligence Council/ Office of the Director of National Intelligence

Camino Kavanagh, Visiting doctoral fellow (King's College), Canada Centre for Global Security Studies, U. of Toronto

Mitchell Kamoroff, Director, Trusted Mission Systems and Networks, DOD

Franklin Kramer, Distinguished Fellow, Atlantic Council

Karl Levitt, Professor, Electrical Engineering & Computer Science, University of California at Davis

Patrick Lincoln, Director, Computer Science Laboratory, SRI, Palo Alto, CA

Adriane Lapointe, Special Assistant for Cyber to the Director of Foreign Affairs, National Security Agency

Herbert Lin, Program Director, National Academy of Science/ National Research Council, Washington, DC

Kristin Lord, Vice President & Research Director, Center for a New American Security, Washington, DC

.

Catherine Lotrionte, Professor & Executive Director, Institute for Law, Science & Global Security, Georgetown University

John Mallery, Research Scientist, Computer Science and Artificial Intelligence Laboratory, MIT

Michele Markoff, Senior Policy Advisor, Office of the Cyber Coordinator, US Dept of State

Tim Maurer, Harvard Kennedy School of Government, Harvard University

David Mussington, Senior Advisor for Cyber Policy, Office of the Secretary of Defense, (Us) Dept. of Defense

Jan Neutze, Senior Security Strategist, Office of Global Security, Strategy and Diplomacy, Microsoft Corporation

Vinh Nguyen, Senior Analyst, US Department of Defense

Joseph Nye, Professor, Harvard Kennedy School of Government, Harvard University

Christopher Painter, Coordinator of Cyber Issues, US Dept. of State

Greg Rattray, Partner Delta Risk

Karl Frederick Rauscher, Chief Technology Officer, EastWest Institute

Rafal Rohozinski, CEO, SecDev and Senior Fellow, Canada Centre, U. of Toronto

Dr. John Savage, Professor, Computer Science, Brown University

Michael Sechrist, Project Manager, Minerva Research Initiative, Harvard Kennedy School of Government, Harvard University

Michael Siegel, Research Scientist, Sloan School of Management, MIT

Admiral (ret.). William (Bill) Studeman, independent consultant

.

Eneken Tikk, Head, Legal and Policy Branch, NATO Cooperative Cyber Defense Centre of Excellence, Tallinn

Paul Triolo, Senior Analyst, US Dept. of Defense

Jody Westby, CEO, Global CyberRisk and Distinguished Fellow, Carnegie Mellon CyLab

Pano Yannakogeorgos, Military Analyst, Air Force Research Institute, Montgomery, AL