Panel 7: Alternative Lenses and Models for International Norms and Governance

Roger Hurwitz, chair and rapporteur
Martha Finnemore, Yurie Ito, Alex Klimburg, Sarah McKune, Emilian Papadopoulos

This panel explores the possibilities, possible contents and levels of impact of norms initiatives by or for non-state actors, including private sectors, civil society, cyber security practitioners and even loosely organized individuals. Such interested third parties may include IGOs that develop a supra-national interest in stabilizing and maintaining cyberspace.

Below are the framing questions for the panel:

1. What is the logic for regional cybersecurity alliances in the supposedly borderless world of cyberspace? Do such alliances have interests and constituencies that in some sense transcend those of the individual member states? May there be some recognition that the notion of a "common problem" is that of a shared problem, because of interdependence, more than each state having the same problem?

2. Are norms and best practices at the operational level, e.g., an ethos of cooperation among national CERTs, a basis for influencing practices and potential norms at state and international security policy levels? Alternatively, to what extent is cooperation and trust at operational levels put at risk by behaviors of state actors?

3. The private sector, especially ICT vendors, Tier 1 carriers and major online services have considerable roles in shaping cyberspace. As a group, their interests and drivers might conflict with those of states. What freedom might some have for an initiative that sets out their own norms of use and misuse of cyberspace? What effect could this have?

4. NGOs and other members of international civil society (INGOs) typically have an interest in the free flow of communication. Some have been targets of cyber attacks by state actors, and some have received material aid from other states. What norms, e.g., export controls on surveillance and filtering technologies, might they advocate? Can they align with some states in promoting these norms, while not losing independence of state interests or their credibility? What might be appropriate forums for pursuit of their interests?

5. What has been the success in other domains and issues of interested third parties developing their own norms and getting state actors to adopt some? What conditions enable success and which block it. Is the abolition of the slave trade a relevant example or the more campaign against land mines? Or might the limited success of the environment movement be more relevant?

6. A decade ago, Chris Kelty wrote about "recursive publics" in cyberspace, i.e., online groups that discussed and created/ maintained the online conditions that

allowed them to discuss and create/maintain the online conditions… They were norm entrepreneurs, after a fashion, but perhaps possible only in the cottage industry phase of cyberspace. Can such loosely organized groups still help shape cyber norms?

Summary

The questions for this panel addressed the possibilities for the development and promotion by non-state actors of cyber norms which could gain significant traction on a regional or global level. Such actors might be regional IGOs, e.g., the OSCE, with supra-national goals, interested third parties in the private sector, such as multi-national ICT vendors, or civil society, and even smaller, loosely organized groups – "recursive publics" – concerned with maintenance and development of the Internet and cyberspace. There are multiple premises for such questions.

Conditions specific to the Internet itself suggest that non-state actors and supra-national actors can influence states regarding adoption of norms. These conditions include

a) Private sector ownership of the physical substrate of the Internet;
b) Governments' dependence on multi-national vendors for maintenance and development of their vital cyber based operations;
c) The increasing role of cyber in economic growth and well being of states;
d) Network based interdependence that vitiate cyber defenses based only on national capabilities;
e) Significant differences among states, the private sector and civil society in their interests and threat perceptions with regard to cyberspace.

In addition, over the last half-century, campaigns originating in civil society to establish global norms for human rights, land mine abatement, the environment and other causes have succeeded to varying degrees in influencing state policies and behaviors.

Much of the success has been due to new information technologies, including, of course, the rise of the Internet and build out of cyberspace: These enabled rapid collection and dissemination of information on the conditions the activist sought to ameliorate and lowered transaction costs in mobilizing public opinion in support of proposed norms.

The panel's apparent consensus, however, was that non-state actors whether private sector entities, NGOs or recursive publics are unlikely to promote and gain adherence to norms of their own at a global or significant regional level. While such groups may influence states' support for particular cyber norms or affect their implementations, some of their current practices – their own operational norms – could be threatened by states' involvement in cyberspace that reduces their independence of action.

Likewise, cyber interdependence has not fostered the development of supra-national interests in cyber defense or development. Even when states are linked for such matters through existing regional organizations, e.g., NATO, OSCE, many have sought to structure their external relations in these matters through a series of bilateral agreements

with other states. These trends support the argument that a Westphalian system is being introduced in cyberspace, characterized by states' self-assertion at political and jurisdictional levels and, as noted in panel 2 discussions, by territorializing at operational levels, i.e., reduction in number of international gateways, redirecting packets addressed directed beyond national borders to pass through routers under government control.

On Regional Alliances

(Panelist 1) National CERTs in various regions of the world have created frameworks for collaboration with different primary foci, according to common concerns in their regions. The alliance of African CERTs is focused on the problem of operating under constraints in funding and capacity, collaboration among CERTs in Muslim countries is primarily focused on handling controversial contents, with cyber security having a low priority, and the Latin American CERT alliance is focused on information sharing to combat cybercrime. Until recently, cooperation among Asian Pacific CERTs seemed motivated by a shared vision of a clean Internet and focused on cleaning up Botnets.

The collaboration among CERTs is built on trust and can sometimes be threatened by tensions among states especially when a country's national CERT is closely tied to its government. For example, the disclosures about the US's Olympic Games program have raised fears in some CERTs that technical information shared for cyber security might by used by a state for military intelligence or competition purposes. One response has been discussions among CERTs for a norm of clearing separating "security operations" from the "intelligence and competitive domains," in order to protect the trust basis of collaboration.

Another example of the challenge from interstate tensions is the very recent political conflict among China, Japan and Korea, over the South China Sea. A number of scheduled meetings among their governments' officials have been cancelled, but fortunately the trust among their respective CERTs has proved robust enough to the technical collaboration to continue working. As states try to take greater roles in governing the Internet, these examples highlight that the private sector and technical groups will be even more important in maintaining trust and collaboration operational levels of the Internet.

(Panelist 2) Operational level collaboration among EU states for cyber security appears increasingly on the basis of bilateral or mini-lateral negotiations, without the guidance of an overall regional vision. Even a regional institution, like NATO, has not defined its collaborations according to such a vision, but has pragmatically opened up its cyber security and cyber defense planning to non-NATO states. The absence of a regional vision with regard to cyber security may also be suggested by NATO's reluctance to declare its Article 5 – collective security – applicable to the defense of cyberspace, but instead to see cyber-attacks as matters for consultation – Article 4 – on a case by case basis, to which member states could independently support the state under attack.

(Panelist 3) Collaboration for cyber security in the Shanghai Cooperation Organization (SCO) occurs in the context of an organization focused heavily on security cooperation and founded on principles of national sovereignty, territorial integrity and opposition to the three evils of terrorism, separatism and extremism.

The SCO agreement on cooperation in the field of international information security (2009) regards any dissemination of certain "harmful" content, as well as use by states of the information space to "undermine" political, economic and social stability in other states, as threats to security. It calls upon states to jointly monitor and respond to such threats. The motive for cooperation is no higher than that of state interest or regime preservation, but it is this clear, common understanding of the similarity of threats to them that enables the states to cooperate. The norm of responding to such perceived threats is also supported by these states' general disinterest in distinguishing between online actions that are political versus genuinely criminal in nature – an ambiguity that facilitates the norm being observed at operational levels.

What roles for the private sector in the development of cyber norms?

(Panelist 4) It is important to have the private sector participate as informed voices in the discussion and development of norms: the private sector holds significant technical expertise, owns much of the critical infrastructure that underlies national economic and security interests, can operate quickly to implement norms, and has significant economic interests at stake in the stability of cyberspace. Even more important, perhaps, is the private sectors' important role in implementing, rather than just articulating, norms. Thus the US Securities and Exchange Commission (SEC) can promote a norm of information sharing on security breaches by requiring a public company to disclose a breach that materially affects the company's business, yet the SEC may not know when a breach has occurred and has limited power to enforce the norm by penalizing a company for failure to disclose. So, for a norm to disclosure to gain traction, the private sector must have a positive attitude toward it and seek to implement it.

The history of environmentalism perhaps provides a useful model, since many companies have accepted and even innovated environmentally friendly practices, often after resistance to government regulation but incentivized by public opinion, leverage from investors, or legal action.

Discussion: There are several ICT sector initiatives that include Microsoft and some other large vendors to promote norms for secure communications and reducing vulnerabilities in code, e.g., Safecode (http://www.safecode.org/index.php). It has taken some time for the companies involved to work out the bylaws and legal frameworks for such initiatives, because information sharing is involved and some IP might be at risk. But it is important that there be clarity about what the initiative wants to accomplish, about the norm it wants to promote.

(Panelist 5) Technical expertise can be crucial in both persuading states to accept new norms and implementing them. As demonstrated by the development of regimes for the

control of nuclear weapons, technical experts who meet regularly and have access to government officials can have considerable leverage in changing people's thinking about an issue – about the risks and benefits. Teaching to support the adoption of a new norm cannot stop at the top level, but must extend down through several layers of government so that implementation is effective. Expertise also supports implementation by facilitating capacity building and providing technical assistance. Thus when the US government wants another government to comply with a norm, it usually buys it, i.e., offers incentives and provides technical experts, so the other government has both the will and the capacity to comply.

Changes in norms on the global level, such as those discussed for cyber will require changes in the incentive structure and investments in countries' capacities. The US and other states that favor these norms must give other states the packages and teach them, because efforts to impose the changes from the outside will be intrusive and resisted. The Chinese understand this and attempt to get inside governments' decision making circles to get rules written in ways that benefit them.

Discussion: An important point about the learning of norms for nuclear weapons, which might be applicable to cyber norms, is that some learning and associated changes in behavior occurred even before there were contacts and meeting between the US and the Soviet Union on the matter. That should call attention to how governments learns, that is, the mechanisms used. One of these is interactions and contacts through third parties. In the nuclear case, there was the creation of Pugwash conferences, starting in 1957, which solicit ideas from Americans and Soviet officials and used ideas from the former to influence position of the latter. There is also the use of informal contacts between officials ("corridor politics") or track 2 processes, when it is apparent that formal meetings of high ranking officials will not bring a change in anyone's mind. The ideas and analyses from think tanks also contribute to learning by governments, and, for cyber, bodies like the CERTs and the IETF can play similar roles. The interesting questions for cyber is how much of the learning might be structural – a response by groups to perceive constraints on their activities in cyberspace, and whether norms might be more quickly promoted through (the formation of) epistemic communities that see the world the same way.

Response: There are many ways of learning, including structural and self-taught learning, but teaching is also very important in socializing people to the norm, because it is a social relationship. And the nuclear case is relevant here, because the US and the Soviet Union taught other states by example. The US and Russia might do the same for cyber by agreeing quickly on bilateral confidence building measures.

What roles for NGOs in the development of cyber norms?

(Panelist 3) NGOs have often been targets of cyber threats and attacks, particularly from SCO nations. These have led some NGOs, e.g., the Tibetan human rights organizations, to create norms for their own communities through campaigns to raise awareness of cyber threats and the need for cyber hygiene. More broadly speaking, NGOs would like

liberal governments to include protection of civil society in their cyber security strategies, to advocate that states practice restraint in cyber espionage, and to encourage the promotion and protection of international human rights in the online space.
Given the potential utility of governments' leadership on these issues, similar structures and solutions suggested for government and private sector partnerships might be applied to government partnerships for NGOs, e.g., information sharing and participation in RAND-like centers for cyber strategy development. In any case, many NGOs would like a voice in governments' discussion of cyber strategies and an opportunity to demonstrate the relevance of their concerns. Although some organizations such as Citizen Lab have highlighted that relevance, the NGOs need invitations from the governments to join key security-related discussions, which they typically have not received.

Role of recursive publics in norm promotion?

(Panelist 2) As defined by Chris Kelty, recursive publics are "vitally concerned with the material and practical maintenance and modification of the technical, legal, practical and conceptual means of its own existence as a public. It is a collective independent of other forms of constituted power and is capable of speaking to existing forms of power through the production of actual alternatives." Cyberspace has afforded the self-organizing of many such groups; some being black – illegal or criminal -- in character, while other are grey or white. Grey groups, such as hackers of Botnet C&C's, and white groups, often provide services and innovations benefiting more institutionalized cyber players and might have some influence in discussions of cyber policies.

What all the recursive publics have in common and what is basic for their self-production (recursion) is in-group trust. Arguably such trust is a specification for the respective groups of the trust that is a basic component of the end-to-end principle of the Internet – that packets sent will be delivered to their destinations without interference – a principle which is increasingly threatened by some state behaviors. In addition, these groups also committed to the survival of the Internet, preferably in non-fragmented form. This observation applies even to the criminal groups, because as parasites they need the host to survive, albeit not in particularly good health, in order to survive themselves. But their interest, influence and means in advocating for online trust and the unity or openness of the Internet varies over the groups.

Discussion: The model of recursive publics is a good one for thinking about technical bodies, but the sociology of the group should not be split off from the technical work they do, because the members' knowledge of the technical issues generates their trust and respect for one another, as evident in open source communities. Several institutions have recognized the innovative potential of such groups. The US Department of Homeland Security (DHS) through Georgia Tech is funding a program for open source development of security software and practices, and a similar program is operating in the Netherlands.

There are many differences among recursive publics, even among those of the same type, viz., black, grey or white. Some can be easily captured by outside actors, so maintaining their independence may be a key for their effectiveness and influence on others. An

analogy to the Comprehensive Nuclear Test Ban Treaty (CTBT) is useful. For many years, states raised problems of verification to stall progress toward a treaty, but in the meantime scientists were working together to develop a monitoring capability. So once states found a will for a treaty, there was a solution at hand for the verification problem. The application to cyber might be in a network of groups, including CERTs and some recursive publics, which would monitor the health of the Internet. However for such monitoring to be effective and credible, it must be public and seen as independent. Universities have a critical role to play as hosts for some of the groups.

For citation: R. Hurwitz, rapporteur, Summary for Panel 7: Alternative lenses and models for international norms and governance. Cyber Norms Workshop 2.0, Sept., 2012. http://citizenlab.org/cybernorms2012/