CYBERDIALOGUE2012

WHAT IS STEWARDSHIP IN CYBERSPACE?

MARCH 18 - 19, 2012 | TORONTO, CANADA

CYBER DIALOGUE 2012 BRIEFS: WITHER "RULES OF THE ROAD" FOR CYBERSPACE?

Discussions and debates over international norms for cyberspace have increased over the past few years. The growing willingness of states to participate stems from a growing sense of insecurity about threats in cyberspace: cybercrime, cyber attacks on critical infrastructures, political and industrial espionage, cyber-enabled terrorism, cyber-enabled regime-threatening protests; widespread restrictions of Internet use; and the proliferation and affordability of the means to achieve these.[1]

The discussions have, however, revealed a wide geopolitical gulf, blocking consensus on what shared norms in cyberspace might look like. Positions are solidifying around two very different visions marked by strong ideological undertones. Indeed, to many stakeholders/observers, the current situation represents a battle over values: the value of an open, democratic cyber commons on the one hand versus a closed state-dominated architecture on the other. The Internet has become the strategic and operational centre of gravity in this battle, while states are using different instruments of power and persuasion to shape or control it.

National cyber-security strategies have mushroomed, particularly in the West. Conferences and seminars on cyber-security and warfare, cyber crime, cyber espionage, Internet freedom, and Internet governance are being used as platforms to shape common national positions and to form "coalitions of like-minded countries" to achieve strategic cyber outcomes. Each camp takes positions on the basic normative architecture, political-military issues, and perceived Internet threats. Given the shape of current debates it appears that some if not many classical North-South/East-West ideological/economic fault lines are extending to cyberspace.

1 Roger Hurwitz, A Preliminary Report on the Cyber Norms Workshop, MIT, 2011. The Workshop was jointly organized by MIT, Harvard, and the University of Toronto's Canada Centre for Global Security Studies.

A plurality of market economies, largely spearheaded by the US, envisage cyberspace as a "global commons," a domain open to all.[2] Free access enhances the rights of, and connectivity between citizens across the globe. It also drives economic growth in developed nations, and offers economic development possibilities in less wealthy nations.[3] This vision of cyber space emerged from what is often presented as a bottom-up, largely hands-off, nongovernmental, multisector approach to Internet governance, and is underpinned by principles of democratic governance and respect for human rights, open trade, and especially freedom of and access to information. Limited "light touch" regulation of the Internet is the backbone of the strategic narrative informing this vision. Thus multilateral initiatives around standards and regulations such as those propagated by the International Telecommunications Union (ITU) are not welcomed. Countries with a strong history of or aspirations to liberal democratic political systems tend to share this vision.

On the political-military front, this grouping of principally Western countries generally holds that the existing Laws of Armed Conflict (LOAC) apply to cyber-related conflict and therefore in principle reject a new treaty on cyber-related political-military threats.[4] Rather, they posit, further discussion might be required on the applicability of certain provisions of the LOAC to the more complex aspects of cyber.[5] The US estab-

2 Prior to 2010, the US had largely shunned international cooperation around cyberspace, and particularly on the subject of norms. Indeed, a recent report of the National Research Council on Deterrence in Cyberspace lamented that "for over a decade ... the US government while complaining about cyber attacks, espionage and exploitation by other states has avoided international arrangements that go specifically beyond obligating a group of predominantly European states to criminalize and cooperate in prosecuting specified norms of conduct." This strategic posture shifted with the Obama administration and the adoption of strategies such as the US International Strategy for Cyber Security, which calls for much stronger international collaboration in this area. Abraham D. Sofaer, David Clark, and Whitfield Diffie, "Cybersecurity and International Agreements" in Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy (Washington DC: National Research Council, 2010).

3 US Secretary of State, Hillary Rodham Clinton, Internet Freedom speech, January 2011.

4 Hurwitz (p.3)

5 US Vice-President Biden clearly laid down the US position regarding the applicability of the LOAC at the London Conference on Cyberspace, noting that many countries believe in and join the US position on the issue. The proceedings of the high-level norms workshop hosted by MIT, Harvard and the Canada Centre for Global Security Studies note that "in practice there is insufficient experience with the use of cyber in warfare 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 the applicability of LOAC in the kinetic world."(p.3) Hurwitz, 2011. Also, in 2010, a WSJ reporter already noted that the US believes a treaty to be premature on the basis that it would not prevent countries like Russia and China from using third parties to circumvent the treaty (Maurer 2011).

lished a Cyber Command in 2010 and other states are following suit, increasing their investment in military cyber capabilities, notwithstanding the current financial climate. Similar arguments are tabled by the group regarding frameworks for responding to the use of the Internet by terrorists or organized criminal networks. In light of the challenges posed by the growing and costly incidences of cybercrime, the same group argues that while the European Convention on Cybercrime requires revision, it should be expanded to cover all states and enable much more effective cross-country collaboration in the fight against cybercrime.[6]

On Internet freedom and the broader debates on governance of cyberspace, the group holds strongly to democratic principles and human rights. The United States is leading a full-blown diplomatic foray with European allies including the EU, the Netherlands, Sweden, and the UK to ensure that these norms are socialized through what US Secretary of State Hilary Clinton has referred to as "patient, persistent and creative diplomacy."[7] The US, UK, Australia, Canada, Germany, the Netherlands, Sweden, and others have adopted national cyber-security strategies strongly underpinned by democratic norms and principles and a commitment to reaching consensus on what global norms for cyberspace should look like. Other developments include the G8 Declaration on Renewed Commitment for Freedom and Democracy of May 2011;[8] the OECD Principles on Internet Policy-Making, adopted by some thirty-four OECD countries, plus Egypt in June 2011;[9] the Council of Europe Declarations on Internet

6 The 2011 workshop on norms in cyberspace noted that "the formulation of subsequent norms would 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 cooperation of relevant publics and stakeholders; the possibility that police work is structurally unable to reduce cybercrime" (Hurwitz, 2011, p.5).

7 US Secretary of State, Hillary Clinton, Keynote address at the Google Big Tent event ahead of the Internet Freedom Conference hosted by the Government of The Netherlands, December 2011.

8 The principles agreed upon "[include] freedom, respect for privacy and intellectual property, multistakeholder governance, cyber-security and protection from crime that underpin a strong and flourishing Internet." G8 Declaration - Renewed Commitment for Freedom and Democracy, G8 Summit of Deauville, 26-27 May 2011. Note on criticism of the Declaration - ref. Article 19.

9 The OECD principles include: promoting and protecting the global free flow of information; promoting the open, distributed, and interconnected nature of the Internet; promoting investment and competition in high-speed networks and services; promoting and enabling the cross-border delivery of services; encouraging multistakeholder cooperation in policy development processes; fostering voluntarily developed codes of conduct; Developing capacities to bring publicly available, reliable data into the policy making process; ensuring transparency, fair process, and accountability; strengthening consistency and effectiveness in privacy protection at a global level; maximizing individual empowerment; promoting creativity and innovation; limiting intermediary liability; encouraging cooperation to promote Internet security; giving appropriate priority to enforcement efforts.

Governance Principles and on the Protection of Freedom of Expression and Information and Freedom of Assembly and Association with regard to Internet domain names and name strings adopted in September 2011, as well as the related recommendations to member states on the protection and promotion of the universality, integrity, and openness of the Internet;[10] the cyberspace principles tabled by UK Foreign Minister William Hague at the London Cyber Security Conference in October 2011;[11] and the Hague Declaration on Internet Freedom, signed by some fifteen like-minded states in December 2011.[12]

A second set of countries has coalesced around a more top-down, territorial vision of how cyberspace should be governed. This vision is underpinned by the principle of state sovereignty enshrined in the UN Charter. At the international policy level, its proponents are more focused on "trying to create the norm of the state as the final arbitrator of the Internet within a specific territory," establishing territorial-like borders in cyberspace as a means to control both the content and flow of information. Access to information and freedom of expression, particularly through online social forums, are seen as a threat to state power rather than a democratic right. A state-controlled Internet is at the core of this vision. Changes to the Internet architecture should be implemented through national laws and policy and state-sponsored technological tinkering. The International Telecommunications Union (ITU) is considered by

10 The CoE principles focus on i) protection and respect for human rights, democracy, and rule of law; ii) assurance of multistakeholder governance; iii) responsibilities of states vis-à-vis Internet-related public policy that respects Internet freedoms and the rights of individuals; iv) the global nature of the Internet and objective of universal access; vi) the integrity of the Internet; vii) decentralized management; viii) open architecture; ix); Network neutrality; and x) cultural and linguistic diversity.

11 The seven principles were presented in Hague's opening speech as follows: the need for governments to act proportionately in cyberspace and in accordance with international law; the need for everyone to have access to cyberspace, including the skills, technology, confidence, and opportunity to do so; the need for users of cyberspace to show tolerance and respect for diversity of language, culture, and ideas; ensuring that cyberspace remains open to innovation and the free flow of ideas, information, and expression; the need to respect individual rights of privacy and to provide proper protection to intellectual property; the need for us all to work together collectively to tackle the threat from criminals acting online; and the promotion of a competitive environment which ensures a fair return on investment in networks, services, and content.

12 The declaration was endorsed by Austria, Canada, the Czech Republic, France, Estonia, Ghana, Ireland, Kenya, the Republic of the Maldives, Mexico, Mongolia, the Netherlands, the United Kingdom, the United States, and Sweden. Commitments included i) establishing a coalition for information sharing, including on violations and other measures that undermine freedom of expression and other human rights on the Internet; ii) collaboration to support politically and through project aid, the realization of individuals' rights, particularly in repressive environments; and engagement with other stakeholders;; iii) bilateral and international cooperation and diplomacy; iv) engagement with ICT businesses to encourage against adoption of policy and practices that may undermine Internet freedoms and individual rights.

this group to be "the appropriate agency for Internet governance."[13] Countries with a strong history of autocratic governance tend to share this vision.

On the political-military front, this group of states, while significantly more politically, economically, and culturally diverse than the US-led group, argues for some form of cyber arms control as an indirect means to level the technological, and by extension, military and economic playing fields. Since 1998, Russia has spearheaded the adoption of consecutive resolutions on various cyber-related challenges within the First Committee of the UN General Assembly, counting on the unfettered support of China, the country that enforces the most sophisticated on-line surveillance and filtration systems in the world, as well as less technologically developed countries.[14] For many years, the US consistently rejected these resolutions. Unfettered, in September 2011, a group of countries led by Russia and China tabled an "International Code of Conduct for Information Security" for consideration at the next session of the UN General Assembly, arguing that the increasing militarization of the Internet [by Western nations] propelled the decision to propose the code.[15]

Also in 2011, the Russian MFA released a "concept for a Convention on International Information Security" at the Second International Meeting of High-Ranking Officials Responsible for Security Matters in Yekaterinburg, Russia.[16] It is engaging in high-level meetings with countries such as India on the merits of the concept, which apparently has the support of some fifty-two countries. Both the code of conduct and the draft convention include provisions banning the use of the Internet for military purposes

13 Hurwitz 2011. In 2010, China for example, noted in a White Paper on Internet Policy that the UN should be given full scope in international Internet administration (Maurer 2011).

14 Among the most important of several General Assembly resolutions on this subject is no. 55/63 which recommends establishing a set of universally agreed-upon principles for the use and protection of cyberspace; understandings by governments as to their responsibilities regarding their resort to cyber attacks or investigations; agreements by governments as to private activities that should be prohibited to enhance cyber security; commitments by governments to criminalize, prevent, investigate, prosecute, and punish such activities; commitments by governments to provide forensic cooperation in cyber investigation and prosecutions by other governments, and to extradite or prosecute violators of agreed norms; agreements among states to allow within their territories certain types of investigation of cyber attacks by other governments; consideration and implementation through an agreed entity of protocols and standards designed to enhance cyber security; and the collective development and funding of an effective, multilateral program of support for cyber competence and capacity throughout the world to facilitate development and economic growth while instilling proper practices (NRC 2011).

15 The code of conduct was proposed by the Permanent Representatives of China, the Russian Federation, Tajikistan, and Uzbekistan (A/66/359).

16 http://rusemb.org.uk/policycontact/52.

and for the overthrow of regimes in other countries, again with the unspoken aim of countering the threat of US cultural influence and military superiority in the domain.[17] Adoption of the texts would assure that individual countries would assume their own sovereign roles with respect to cyberspace policy; and while provisions on freedom of expression and access to information are included, so are follow-on caveats that render these rights contingent on national security.[18] Indeed, and as noted by Russian information security expert Andrey Krutskikh, "ensuring information security must not suppress freedom; exercise of freedom must not jeopardize national security and sovereignty."[19] The Shanghai Cooperation Organization 2009 Agreement on Information Security, which came into force in 2011, shares similar provisions, as do several of the agreements shaping high-level ICT strategy and policy in the countries of the Commonwealth of Independent States (CIS). Meanwhile, Russia and Brazil have signed an accord similar to the SCO 2009 Agreement. High-visibility incidents such as Stuxnet and the important role social media played in the political upheavals in the Arab region have only served to reinforce this narrative.

The ITU is the international channel through which this group of countries aspires to deliver its state-dominated version of Internet cyberspace. While this year's World Conference on the Internet (WCIT-12) (which will largely focus on reviewing the ITU foundational treaty) might not turn out to be a strategic win for this group given how the US has purportedly played its cards, the build-up has certainly raised the hackles

17 Remarks by Russian MFA representative A.Krutskikh at London Cyber Conference, Nov. 2011.

18 Both texts also note that states should protect freedom of expression on the Internet and "have no right to limit citizens' access to information space," with the caveat that governments may, however, limit these rights "for the protection of national and public security." The draft Convention specifically calls on states to abstain from using information and communication technologies to interfere in the internal affairs of another state and "to abstain from slanderous statements, abusive or hostile propaganda for the implementation of intervention or interference into the internal affairs of other states.

19 Remarks by Russian MFA representative A.Krutskikh at London Cyber Conference, Nov. 2011.

of the public and private sectors and Internet rights activists in the West.[20] [21]

Regarding cybercrime, a broader group, which includes Brazil and South Africa, is opposed to accession to the Budapest Convention and has been pushing for the negotiation of a new cybercrime treaty under the auspices of the United Nations. Russia itself has rejected a portion of the Convention on the grounds that it "violates their Constitution by permitting foreign law enforcement agencies to conduct Internet searches inside Russian borders"[22] At the regional level, initiatives aimed at responding to cybercrime have been adopted by the ASEAN Regional Forum, the CIS, and the SCO, some of which include collaboration with countries in other regions.

A CASE OF NEVER THE TWAIN SHALL MEET?

The different strategic narratives that have emerged around rules of the road for cyberspace are marred by internal contradictions. For example, while the Russian Federation is pushing for a state role in the governance of the Internet, as a member of the G8 and member state of the Council of Europe, it is simultaneously signing up to a range of principles that promote the complete opposite. Meanwhile, the debate over who or what body should govern the Internet remains complex, not least in relation to domain names. While ICANN is presented as a 'bottom-up', non-governmental entity based in the U.S., "it still remains under the purview of the U.S. government, specifically the Department of Commerce."[23] The US government "attempts to influence the operations of this institution for its own economic ends," provoking the

20 http://online.wsj.com/article/SB10001424052970204792404577229074023195322.html

21 In January 2012, the US government issued a memo to private companies noting that it was aware of concerns that WCIT-12 would be a "battle over investing the ITU with specific [Internet] governance authority," but made clear that the conference "poses no threat of a "takeover of the Internet by intergovernmental institutions." The memo explained how the US had forestalled this eventuality by developing a detailed WCIT-12 position "that pushed to make the existing IT Regulation (ITRs) the basis for treaty negotiations" and by extension, sought to achieve further liberalization and deregulation. According to the same memo, the strategy was successful since the ITRs were accepted as the framework for negotiation, therefore ruling out the threat of the ITU taking on ICANN-like Internet governance authority, At the same time, the memo cautioned that preparation should be made since foundational issues are most likely to be raised anyway at the meeting in Dubai.

22 Gorman cited in Tim Maurer, "Cyber Norm Emergence at the United Nations: An Analysis of the Activities at the UN Regarding CyberSecurity" (Harvard Kenney School, Belfer Center for Science, and International Affairs, 2011).

23 David J. Betz and Tim Stevens "Power and Cyberspace," in *Cyberspace and the State: Toward a Strategy for Cyber-Power* (London, Adelphi Series, 2011), 424, 35-54

suspicion, if not animosity, of governments and other stakeholders across the globe.[24] Some countries from the European Union are also in favour of replacing ICANN with an intergovernmental group, leading the US to finally compromise in 2009, and accept the creation of the Internet Governance Forum (IGF).[25] The IGF, which was launched at the World Summit on the Information Society in Tunis, Tunisia, would allow governments to "debate and make recommendations about Internet policy issues but not exercise direct policy authority."[26] Yet, as Jonathan Zittrain notes, "such efforts import from professional diplomacy the notion of process and unanimity above all. Their solution for the difficulties of individual state enforcement on the Net is a kind of negotiated intellectual harmony among participants at a self-conscious summit— complex regimes to be mapped out in a dialogue taking place at an endlessly long table, with a role for all to play. Such dialogues end either in bland consensus pronouncements or in final documents that are agreed upon only because the range of participants has been narrowed."[27]

In October 2011, India, the largest democracy in the world, tabled a proposal at the UN General Assembly for the establishment of a UN Committee for Internet-related policies (CIRP). The proposal built on the earlier Geneva Declaration of Principles and the Tunis Agenda with regard to Enhanced Cooperation, as well as the outcome of the 2011 IBSA stakeholder meeting on Global Internet, endorsed at the 2011 IBSA Summit in Durban, South Africa. The CIRP proposal sparked an outrage, with many alleging that it constituted *inter alia* a "UN takeover of the Internet." Some observers posit that important contradictions emerge in the main justifications for opposing such transnational initiatives. Justifications are generally centered on the somewhat naïve assumption that free-flowing multistakeholder networks currently govern the Internet. The choices are presented in black and white and offer no alternatives: either we maintain the bottom-up decentralized regime of governance or we hand it over for governments to control. And as noted, they are also centered on the erroneous view that the

24 Ibid

25 Tension had been mounting around the Internet governance debate since the 2005 Tunis Agenda on Enhanced Cooperation. The relevant working group had recommended inter alia, that a new global body be established within the UN system to oversee Internet governance-related policy.

26 Maurer 2011.

27 Jonathan Zittrain, *The Future of the Internet and How to Stop It* (New Haven, CT: Yale UP, 2008).

US engages in hands-off stewardship of Internet governance.[28]

While the US and like-minded states are pushing to keep the Internet free from state control, some argue that they have actually "failed to develop a coherent strategic narrative in which defense and development of the Internet are assured, nor have they proposed an architectural framework to counter the models proposed by Russia, China and others."[29] The lack of strategic coherence is in part related to the dissonance that exists within and between democratic states on competing "cyber agendas." "Real world" political and bureaucratic turf battles between the justice and human rights camps and the security and national interest camps are playing out over cyberspace, while simultaneously undermining broader strategic narratives. In addition, the vision of Internet architecture and institutions that proponents of the "global commons" continue to cling to might well have fostered technological development and promoted democratic ideals, but "they are now at the end of their life cycle. They do not sufficiently accommodate the shift in Internet demographics to the East and South; they do not give new states a seat at the decision-making table; and they are not accommodating the great, on-going growth wave in mobile and cloud computing."[30]

At the same time, democratic countries are increasingly engaging in the very restrictive behaviour for which they critique others— the spike in how legal and market pressures are being invoked to justify the removal of content from Web hosting and social networking platforms, and the degree to which states are offloading policing activities to Internet Service Providers (ISPs), bear evidence to this trend.[31] Indeed, many democratic countries have passed "far-reaching surveillance measures that enable widespread eavesdropping on e-mail, cellular phone and other communications activities by requiring ISPs to retain, and when required, turn over such

28 For example, the US has intervened in the grant of .xxxgTLD, placed pressure on financial intermediaries to strangle Wikileaks, extra-judicially seized domain names served by US-based registries, and bills such as SOPA, PROTECT-IP, and E-PARASITES have been introduced in the Senate and Congress. IGFWatch news, "India's proposal for a UN Committee for Internet-related Policies (CIRP)", 29/10/2011

29 Hurwitz 2011.

30 Ibid.

31 Ronald Deibert, John Palfry, Rafal Rohozinski and Jonathan Zittrain, *Access Contested: Security, Identity and Resistance in Asian Cyberspace* (Cambridge, MA: MIT Press, 2012), 31-32. See also Frank La Rue, Annual Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Wxpression, A/HRC/17/27 (Section 3)

information to legal authorities."[32] Such actions on the part of democratic governments, coupled with the unbridled influence that ISPs and social-networking companies are playing in public and private matters, are strongly impacting the social contract and political processes.[33]

Furthermore, recognition of cyber as a strategic domain, the Wikileaks incident and high-stake political, industrial, and economic espionage have thrust the issue far beyond the initial concerns regarding cybercrime, piracy, copyright, and child pornography. The political rush to "secure cyberspace" is generating enormous economic opportunities for many companies. However, unlike the dot.com boom of the 1990s, led by companies "seeking to open up cyberspace," the current boom responds to national security spending prerogatives and is moving largely unchecked in the opposite direction.[34] Second, the development of military doctrines and cyber capabilities for operations in cyberspace is not just the purview of China, Iran, or Russia. The US and its allies are leading the current rush, in order to maintain strategic superiority, "silence information that is strategically threatening, and sow confusion and doubt among opponents dependent on cyberspace for information and organization."[35] For other states, the logical response is to either match these capabilities, or undermine them. And thus the cycle continues…

The current debate grows exasperating as the opposite poles fail to edge any closer to a comprehensive set of rules for governing cyberspace. Instead, "many states are unprepared at this time to limit their control of cyber activities they regard as essential to their national interests."[36] At the same time, international agreements remain elusive as long as irreconcilable differences in policies regarding political uses of the

32 Ronald Deibert and Rafal Rohozinski, "Control and subversion in Russian cyberspace," in *Access Controlled: The Shaping of Power, Rights and Rule in Cyberspace* (Cambridge, MA: MIT Press, 2010), 15-34

33 Lori Andrews, *I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy* (New York: Free Press, 2011), chap. 1.

34 Deibert et al., 32.

35 Ibid

36 Sofaer, Clark, and Diffie, "Cybersecurity and International Agreements."

Internet, privacy, and human rights remain.[37] Conversely, while these factors limit the potential scope and utility of comprehensive rules, consensual acknowledgement of the problems can allow for international cooperation on many complex and sensitive issues, eventually proving beneficial to all stakeholders. Indeed, despite the strong differences between different poles on security and freedoms in cyberspace, there are windows of opportunity emerging that might allow for both formal and informal collaboration and confidence-building measures around certain rules and behaviours in the domain.

For example, on the political-military front and after several years of reaching the same impasse on norms in cyberspace, in 2010 the Group of Governmental Experts (GGE) that met within the framework of the UN General Assembly First Committee meetings on the "Creation of a Global Culture of Cybersecurity," agreed for the first time on the scope of the threat and the need to work around a set of confidence-building measures that would include:

1. Further dialogue among states to discuss norms pertaining to state use of ICTs, to reduce collective risk and protect critical national and international infrastructures;
2. Confidence-building, stability, and risk-reduction measures to address the implications of state use of ICTs, including exchanges of national views on the use of ICTs in conflict;
3. Information exchanges on national legislation, national ICT security strategies and technologies, policies, and best practices;
4. Identification of measures to support capacity building in less developed countries; and
5. Finding possibilities to elaborate common terms and definitions relevant to United National General Assembly resolution 64/25.[38]

Subsequently, in December 2011, the UN General Assembly reached consensus on

37 Ibid.

38 The Group of Governmental Experts representing fifteen states, including China, India, Russia, and the US, met four times and on 10 July 2010 issued a report summarizing the threats currently faced by Information and Communication Technologies ("ICTs"), jointly stating that "existing and potential threats in the sphere of information security are among the most serious challenges of the twenty-first century and recommending "further steps for the development of confidence-building and other measures to reduce the risk of misperception resulting from ICT disruptions."

establishing a new GGE to implement these measures and "to continue to study existing and potential threats in the sphere of information security and possible cooperative measures to address them, including norms, rules or principles of responsible behaviour of States and confidence-building measures with regard to information space."[39] The new GGE will present its report to the Secretary-General in 2013. These developments are evidence of an interesting strategic shift in policy vis-à-vis international cooperation on cyberspace, not only in the US but also across states and regions.

Meanwhile on the cybercrime front, the divide between the pro- and anti- Budapest Convention states definitely persists. Here too, however, informal collaboration and cooperation between states is growing and states are open to learning from the positive experiences of collaboration and cooperation that have emerged in the anti-money laundering field.[40] The UN Security Council formally recognized the threat of cybercrime and other forms of transnational organized crime to international security in a presidential statement issued in 2010.[41] The OSCE has included cybercrime as a strategic priority in its area of responsibility and is supporting member states' efforts to respond to cybercrime-related threats through capacity building and related means.[42] The UNODC has also included cybercrime as a strategic priority, while the Commonwealth heads of state recently approved an initiative on cybercrime bringing Commonwealth members closer to the basic tenets of the Budapest Convention. Many of these initiatives are viewed as opening up the space for exercising diplomatic conviction through the tools of capacity building, support for legislative drafting, information, and resource sharing across regions.

These steps are positive, yet remain limited. Significant gulfs still need to be bridged between positions and interests vis-à-vis rules for cyberspace, and particularly the Internet. What next therefore, for the rules of the road?

39 A/Res/66/24 Member states have since proposed experts to the UN-Secretary-General and new GGE will commence its work in spring of 2012.

40 Glenny, IPI meeting on Transnational Organized Crime (closed), NY, February 2011; Christopher Painter, IISS launch of Cyber and the State, Washington DC, January, 2011, http://www.youtube.com/watch?v=NeA3r_s5zCs

41 S/PRST/2010/4

42 *CIC Annual Review of Special Political Missions* (2011). Background paper on OSCE counter-transnational organized crime-related activities.

Prepared by Camino Kavanagh with the support of Matthew Carrieri

---

Camino Kavanagh is currently pursuing a PhD at Kings College London's Dept. of War Studies and is a non-resident fellow at University of Toronto's Canada Centre for Global Security Studies and the Citizen Lab. Her principal research focus is on power dynamics in (and in relation to) cyberspace. Camino is also a Fellow at NYU's Center on International Cooperation (CIC) where she focuses principally on transnational threats such as organized crime and trafficking. She has an MA in Contemporary Warfare and an MA in International Human Rights Law

Matthew Carrieri is currently finishing his MA in Near Eastern Studies with business focus at NYU; and has a BA in Middle East Studies from McGill

ANNEX

Possible norms for cyberspace tabled at a workshop hosted by Harvard Belfer Center, MIT CSAIL, and the University of Toronto's Canada Centre for Global Security Studies.

Norms regarding military operations in cyberspace	Norms regarding political, military, economic, and industrial espionage	Norms for technological foundations for secure cyberspace	Normative bases for public-private partnerships/ defensive coordination	Norms for Internet freedom and a global information society
In principle, LOAC sho¬huld be applied to such 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.	States should recognize the international implications of their technical decisions, and act with respect for one another's networks and the broader Internet	Norm that limits or calls for arrangements that limit (or specifies circumstances for) surveillance and data collection by private companies.	Internet freedom as a global norm – should allow for ambiguity and 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, and de-escalationtt	Regulation of the growing trade in cyber espionage and surveillance services by security and defence contractors in developed countries to authoritarian countries for use against political dissidents	States should act within their authorities to help ensure the end-to-end interoperability of an Internet accessible to all.	Governments should seek cooperation with the private sector to assure a clean and healthy Internet.	
Development of a structural norm (practice) of military involvement in the protection of domestic critical infrastructure from cyber attack (raises questions of RoE when non-state actors are involved)	Norm that ensures that states and other stakeholders educate themselves about cybercrime, including with respect to the hiring of criminal hackers.	States should respect the free flow of information in national network configurations, ensuring they do not arbitrarily interfere with internationally interconnected infrastructure		
Norms that routinize information-sharing, assistance in disaster or attack, cooperation in forensics, collaboration in analysis of attacks.	Encryption of computers and cloud servers to inhibit theft of politically sensitive information (ala Wikileaks)	States should recognize and act on their responsibility to protect information infrastructures and secure national systems from damage or misuse.		
	Distinction between low- and high-impact criminals and expectations for cooperation in the pursuit of high-impact criminals – would require data retention and accessibility for certain types of crime	Globally accepted norms and standards to assure the integrity of the cyber supply chain – would require 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 defence sectors.		
	Duty to warn (or inform) and duty to assist as formalized in some countries through mandatory notification laws and institutionalized at the international level in data sharing procedures among CERTs and NATO allies. Could include encouragement of letters of marque			

BIBLIOGRAPHY

Andrews, Lori. *I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy*. New York, NY: Free Press, 2011.

Betz, David J. and Tim Stevens. *Cyberspace and the State: Toward a Strategy for Cyber-Power*. Abingdon, UK: Routledge, for the Institute for Strategic Studies, 2011.

Biden, Joe. "VP's Remarks to London Cyberspace Conference." The London Conference on Cyberspace. London, UK. 1 Nov. 2011. http://www.whitehouse.gov/the-press-office/2011/11/01/vps-remarks-london-cyberspace-conference.

Cockayne, James, and Camino Kavanagh. "Flying Blind? Political Mission Responses to Transnational Threats." *Review of Political Missions*. New York: NYU Center on International Cooperation, 2011. 19-30.

Council of Europe, Committee of Ministers. *Declaration by the Committee of Ministers on Internet governance principles*. Adopted 21 September 2011 at the 1121st Meeting of the Ministers' Deputies. https://wcd.coe.int/ViewDoc.jsp?id=1835773.

---. *Declaration by the Committee of Ministers on the protection of freedom of expression and information and freedom of assembly and association with regard to Internet domain names and name strings*. Adopted 21 September 2011 at the 1121st Meeting of the Ministers' Deputies. https://wcd.coe.int/ViewDoc.jsp?id=1835805&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383.

Deibert, Ronald, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain, eds. *Access Contested: Security, Identity, and Resistance in Asian Cyberspace*. Cambridge, MA: MIT Press, 2012.

Deibert, Ronald, John Palfrey, Rafal Rohozinski and Jonathan Zittrain, eds. *Access Controlled: The Sharping of Power, Rights, and Rule in Cyberspace*. Cambridge, MA: MIT Press, 2010

G8 Summit of Deauville, 26-27 May 2011. G8 Declaration: Renewed Commitment for Freedom and Democracy. 27 May 2011. http://www.g8.utoronto.ca/summit/2011deauville/2011-declaration-en.html#internet.

Gorman, Siobhan. "US Backs Talks on Cyber Warfare." *The Wall Street Journal*. 4 June 2010. http://online.wsj.com/article/SB10001424052748703340904575284964215965730.html.

Hague, William. "Foreign Secretary Opens the London Conference on Cyberspace." The London Conference on Cyberspace. London, UK. 1 November 2011. http://www.fco.gov.uk/en/news/latest-news/?view=Speech&id=684997682

Hurwitz, Roger. *A Preliminary Report on the Cyber Norms Workshop*. Citizen Lab. Held at the Massachusetts Institute of Technology (MIT), 19 – 21 October 2011. http://www.citizenlab.org/cybernorms/preliminary_report.pdf.

International Institute for Strategic Studies. *Cyberspace and the State*.

Online Video Clip. Youtube. 1 February 2012. http://www.youtube.com/watch?v=NeA3r_s5zCs.

Maurer, Tim. "Cyber Norm Emergence at the United Nations: An Analysis of the Activities at the UN Regarding Cyber-security." Discussion Paper 2010-11, Science, Technology, and Public Policy Program, Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2011. http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf.

McDowell, Robert. "The UN Threat to Internet Freedom." *The Wall Street Journal*. 21 February 2012. http://online.wsj.com/article/SB10001424052970204792404577229074023195322.html.

The Netherlands. Ministry of Foreign Affairs. *Freedom Online: Joint Action for Free Expression on the Internet*. The Hague, NL. 9 December 2011. http://www.minbuza.nl/binaries/content/assets/minbuza/en/the_ministry/declaration-final-v-14dec.pdf/declaration-final-v-14dec.pdf/hippogallery%3Aasset

OECD. *Communiqué on Principles for Internet Policy Making*. OECD High-Level Meeting on the Internet Economy, Paris, France. 29 June 2011. http://www.oecd.org/dataoecd/33/12/48387430.pdf

Rodham Clinton, Hillary. "Keynote Address." Google Big Tent Event. The Hague, NL. 8 December 2011.

---. "Remarks on Internet Freedom." The Newseum, Washington, DC. 21

January 2010. US Department of State. http://www.state.gov/secretary/rm/2010/01/135519.htm.

Russia. Ministry of Foreign Affairs. *Concept of a Convention on International Information Security*. The Embassy of the Russian Federation to the United Kingdom of Great Britain and Northern Ireland, 28 October 2011. Web. http://rusemb.org.uk/policycontact/52.

---. "Remarks by Russian MFA representative A. Krutskikh at London Cyber Conference." The Embassy of the Russian Federation to the United Kingdom of Great Britain and Northern Ireland, 1 November 2011. http://www.rusemb.org.uk/article/112.

Sofaer, Abraham D., David Clark, and Whitfield Diffie. "Cyber Security and International Agreements." *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy*. Washington, DC: National Research Council, 2010.

Terminus [blog]. "India's Proposal for a UN Committee for Internet-Related Policies (CIRP)." *IGF Watch*. 29 October 2011. http://igfwatch.org/discussion-board/indias-proposal-for-a-un-committee-for-internet-related-policies-cirp.

U.N. General Assembly. 17th Session. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*. (A/HRC/17/27). 16 May 2011. http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G11/132/01/PDF/G1113201.pdf?OpenElement.

---. General Assembly, 55th Session. *Combating the criminal misuse of information technologies*. (A/RES/55/63). 22 January 2001. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf.

---. General Assembly, 65th Session. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. (A/65/201). 30 July 2010. http://unidir.org/pdf/activites/pdf5-act483.pdf.

---. General Assembly, 66th Session. *Developments in the field of information and telecommunications in the context of international security*. (A/RES/66/24). 13 December 2011. http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N11/460/26/PDF/N1146026.pdf?OpenElement.

---. General Assembly, 66th Session. *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/66/359). 14 September 2011. http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N11/496/56/PDF/N1149656.pdf?OpenElement.

---. Security Council. *Statement by the President of the Security Council*. (S/PRST/2010/4). 24 February 2010. http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N10/250/67/PDF/N1025067.pdf?OpenElement.

United States. Department of State. *Memorandum: 2012 ITU World Conference on International Telecommunications (WCIT-12), 23 January 2012*. Internet Governance Project, 30 January 2012. http://blog.internetgovernance.org/_attachments/4988735/WCIT-12%20Memo%201-23-12.pdf.

Zittrain, Jonathan. *The Future of the Internet and How to Stop It*. New Haven, CT: Yale University Press, 2008.