SCHOOL FOR INTERNATIONAL STUDIES

Seizing the Diplomatic Initiative to Control Cyber Conflict

Paul Meyer

Simons Papers in Security and Development

No. 45/2015 | September 2015

The **Simons Papers in Security and Development** are edited and published at the School for International Studies, Simon Fraser University. The papers serve to disseminate research work in progress by the School's faculty and associated and visiting scholars. Our aim is to encourage the exchange of ideas and academic debate. Inclusion of a paper in the series should not limit subsequent publication in any other venue. All papers can be downloaded free of charge from our website, www.sfu.ca/internationalstudies.

The series is supported by the Simons Foundation.

Meyer, Paul, *Seizing the Diplomatic Initiative to Control Cyber Conflict*, Simons Papers in Security and Development, No. 45/2015, School for International Studies, Simon Fraser University, Vancouver, September 2015.

ISSN 1922-5725

School for International Studies
Simon Fraser University
Suite 7200 - 515 West Hastings Street
Vancouver, BC Canada V6B 5K3

SCHOOL FOR INTERNATIONAL STUDIES

SFU SIMON FRASER UNIVERSITY ENGAGING THE WORLD

Seizing the Diplomatic Initiative to Control Cyber Conflict

Simons Papers in Security and Development
No. 45/2015 | September 2015

Abstract:
Cyberspace is a unique human-made environment on which global society is increasingly dependent for its well-being. At the same time, states and non-state actors are engaged in detrimental cyber activity that can threaten to transform this special environment into just another battleground. Diplomatic efforts to develop international "norms of responsible state behavior" have not kept pace with growing military cyber security capabilities. A Sino-Russian initiative for an "International Code of Conduct for Information Security" has problematic aspects and could prove divisive if brought before the UN General Assembly for adoption. A series of reports by UN Group of Governmental Experts have generated some important general conclusions and positive recommendations for confidence building measures, but they remain only proposals. There is a need for more Western leadership in ensuring that expert recommendations are transformed into state commitments if the peaceful nature of cyberspace is to be preserved.

About the author:
Paul Meyer is currently an Adjunct Professor of International Studies and Fellow in International Security at Simon Fraser University and a Senior Fellow at The Simons Foundation, Vancouver, Canada. From 1975 to 2010 Paul Meyer was a career diplomat in Canada's Foreign Service with a professional focus on international security policy. He served as Canada's Ambassador to the UN and the Conference on Disarmament in Geneva in 2003–2007.

About the publisher:
The School for International Studies (SIS) fosters innovative interdisciplinary research and teaching programs concerned with a range of global issues, but with a particular emphasis on international development, and on global governance and security. The School aims to link theory, practice and engagement with other societies and cultures, while offering students a challenging and multi-faceted learning experience. SIS is located within the Faculty of Arts and Social Sciences at Simon Fraser University. Our website is www.sfu.ca/internationalstudies.

Seizing the Diplomatic Initiative to Control Cyber Conflict*

Conflict has always been a feature of the international system, and states have devised means of dealing with it along the diplomacy–defense spectrum. Today, however, the international community faces a special challenge regarding conflict in an entirely new domain. Unlike the familiar domains of land, sea, and air, the Internet (more broadly understood as cyberspace) is a human, not a natural, construct that has only existed for some 20 years. Cyberspace constitutes an environment significantly different from other realms of internationally regulated activity. It would be hard to exaggerate its importance for contemporary global society, or the high level of dependency on a cyberspace free from threat of deliberate damage or disruption from state actors.

This dependency reflects the rapid growth of Internet users, recently surpassing the 3 billion mark worldwide, and the exponential increase of participation beyond the original focus of activity in Europe and North America. Today, the majority of Internet users live in the global south. Developing countries have increased their share from 44 percent in 2006 to 62 percent in 2011.[1] Nigeria had approximately 200,000 Internet users in 2002. In 2013, it had 49 million. This wide participation of global populations is ensuring increased government scrutiny everywhere about the public policy implications of the Internet, including the field of cyber security. Although to date much of that governmental attention has focused on countering malevolent action by cyber criminals, the threat of interstate cyber conflict is beginning to emerge as a pressing issue for consideration.

The Issue of State Behavior

Seeking international cyber security through diplomatic means requires taking account of the current relations amongst states. A 2012 survey by the UN Institute for Disarmament Research (UNIDIR) revealed that 114 states have a national cyber security program, and 47 of these assign some role to the armed forces in carrying out that national program. Yet according

* The Version of Record of this manuscript has been published and is available in *The Washington Quarterly*, Summer 2015. See http://tandfonline.com, DOI 10.1080/0163660X.2015.1064709.

to the UNIDIR research, only six states have published military cyber security strategies, with varying degrees of specificity.[2] While these findings point to a lack of transparency in cyber security policies, they also suggest that a certain "militarization" of cyberspace is underway without much public debate on the matter. It is difficult to identify an explicit political decision taken in leading cyber powers to authorize state-sponsored cyber attacks in this new environment, yet they seem to have occurred. **(**for example, the Stuxnet cyber attack against an Iranian nuclear facility in 2009–2010**).** As more information emerges from underneath the cloak of secrecy covering much state-conducted cyber action abroad, an embryonic cyber arms race is emerging.

As is frequently the case with new technology, the United States was an early adopter and has set the pace for others. The U.S. military, for example, created its Cyber Command in 2009 with an initial FY2010 budget allocation for $114 million. Just four years later, its FY2014 allocation is $447 million, nearly a four-fold increase. A similar increase of personnel is also underway with Cyber Command seeking to augment its force by over 4,000 new staffers from the approximately 900 in 2013.[3] Additionally, the Department of Defense in April 2015 released its *Cyber Strategy* to provide policy direction over the next five years. This document attaches great importance to the cyber threat, recalling that the Director of National Intelligence characterized it as the number one strategic threat against the United States. The *Cyber Strategy* foresees the establishment of a Cyber Mission Force of 6,200 personnel when fully operational that will be organized into 133 teams. More disturbing than the expansion of human and financial resources is the emphasis on offensive, in addition to defensive, operations in the underlying strategy. Among the five strategic goals set by the *Cyber Strategy,* one is to "[b]uild and maintain viable cyber options and plans to use these options to control conflict escalation and to shape the conflict environment at all stages."[4] Despite the somewhat opaque military language, the document makes clear that such external force projection would be part of a "comprehensive cyber deterrence strategy" that DOD is to help develop and implement.[5]

Documents released earlier in 2013 by Edward Snowden have provided details of the U.S. policy for offensive cyber operations, as set out in Presidential Policy Directive (PPD) 20 of October 2012.[6] This directive indicates that offensive operations would not be restricted to

countering imminent threats or cyber attacks, but could also seek to advance unspecified national interests. The upper rungs of this cyber ladder of escalation are alarming – cyber effects operations that will result in what the PPD euphemistically terms "significant consequences" allow for actions causing "loss of life" and "significant damage to property," although this level of operations would apparently require presidential approval.

Despite the PPD statement that the United States would conduct any external cyber operations in a manner "consistent with its obligations under international law," it does not really address the major implications of such offensive cyber operations for international security. The policy does acknowledge that among the "risk" factors taken into account for foreign operations are introducing "unwelcome norms of international behavior" or impacting "the security and stability of the Internet." Regrettably, the policy does not indicate a diplomatic dimension beyond referring to a prior call by the Obama administration to develop "an international consensus around norms of [responsible state] behavior in cyberspace."[7]

Snowden's revelation of this policy for offensive cyber operations, alongside the rapid increase in military cyber capabilities, has likely overshadowed the limited earlier appeal to forge a global consensus. As has often been the case in the past, other states are likely to take their lead from U.S. policy and action in determining what posture they should adopt in this new realm of international security. It may represent wishful thinking on my part to hope that this unintended "transparency" measure by the U.S. would lead states (and civil society) to stare into the abyss and question whether they really want cyberspace to serve as just another domain of international conflict. If not, what might be done to preclude, or at least mitigate, its "weaponization?" Any preventive action must be taken in cooperation with other leading cyber powers notably China.

Tense U.S.–Chinese Cyber Security Relations

Even the most casual observer of the Western media should note the growing attention paid to cyber attacks and the losses of information that both public and private entities have suffered. These losses now regularly involve millions of compromised accounts, ranging from personal data of the customers of major corporations to that of U.S. Government employees. In particular, China has been accused of state-sponsored cyber espionage directed at U.S.

government and business interests. After years of discreetly avoiding naming China as the culprit in these cyber attacks, the U.S. government has decided starting in 2013 to identify Beijing as the principal perpetrator and to publicly call upon it to desist

The U.S. Department of Defense has been especially vocal in accusing China in these cyber intrusions, linking them to the compromise of several U.S. weapon systems, including the F-35 and F-18 fighter jets and the PAC3 missile. Former U.S. Secretary of Defense Chuck Hagel has referred to cyber threats as "terribly dangerous" and has called for talks with China and others to "establish international norms of responsible behavior in cyberspace."[8] Indeed, the issue of cyber espionage has figured prominently in U.S.–China bilateral relations and has found its way onto the agenda of the highest levels of discussion, such as the summit between Presidents Obama and Xi in June of 2013 It would appear, though, that the political attention to the problem has not yielded sufficient results.

In May 2014, the U.S. Department of Justice took the unprecedented step of indicting five serving officers of the People's Liberation Army for engaging in cyber espionage against U.S. corporations. Chinese officials have angrily denied these charges and have even suggested that the United States "fabricated" the evidence against the PLA officers.[9] Beijing has also responded to the United States' charges by suspending its involvement in a bilateral cyber working group that had only been recently established.[10] These publicized actions represent a significant escalation over the previous reliance on behind-the-scenes diplomatic protests, and demonstrate the difficulty of sustaining a substantive cyber security dialogue between the two powers.

It is noteworthy that even as the U.S. military moves to significantly enhance its cyber security capacities, the Defense Department is still advocating a cooperative approach to address some potential cyber conflict. The *Cyber Strategy* specifically seeks to strengthen the U.S. cyber dialogue with China in order to enhance strategic stability. It also offers to do the same with Russia "[i]f and when U.S.–Russia military relations resume."[11] This approach looks to diplomatic rather than military initiatives and would ultimately seek to agree on "rules of the road" to govern state behavior in cyberspace. Whether global cyber security will be characterized

by adversarial or cooperative approaches may depend on the near-term success or failure of efforts by cyber powers to develop these norms of responsible state behavior.

The Quest for Norms of Responsible State Behavior

The idea of agreeing upon such norms is not a novel international concept. States have long worked out common standards to cover their interaction, including how to manage conflicts. These agreements have applied to the traditional domains of land, sea, and air, and have evolved to accommodate changes in technology and the introduction of new armaments. However, cyberspace constitutes a unique domain that raises special concerns and considerations for states and their national security establishments.

The United States was the first country to recognize officially the inter-relationship between national and global cyber security and to set out its vision for how the international community should proceed. In May 2011, the Obama administration issued its *International Strategy for Cyber Space*. This path-breaking policy statement acknowledged the immense dependency of society on the operation of networked technologies and the increasing threats to the secure use of these technologies. The policy noted, "Cyber security threats can even endanger international peace and security more broadly, as traditional forms of conflict are extended into cyberspace." To counter this tendency for some states to "exert traditional power in cyberspace," the policy called for a new international consensus on "norms for responsible state behavior" in cyberspace. The statement promised early and energetic action in this regard: "We will engage the international community in frank and urgent dialogue, to build consensus around principles of responsible behavior in cyberspace…"[12]

The policy directions set out in the *International Strategy* are progressive and infused with a cooperative security spirit. But having expressed the goal and stressed the urgency of the requirement, the Obama administration has found it difficult to translate its policy vision into a diplomatic process to achieve it. Although more than four years have passed since its *International Strategy*, the United States has yet to endorse any multilateral process to develop and agree on norms for state behavior, and has struggled to establish or maintain even bilateral dialogues on the issue with key states.

The Sino–Russian Code of Conduct Initiative

Although the U.S. endorsement of the idea of a set of global norms to govern inter-state behavior in cyberspace constituted an important diplomatic step, it was China and Russia that proved first off the mark in presenting a proposal for a package of global norms to govern state behavior. In an official document circulated at the September 2011 UN General Assembly session, the delegations of China, the Russian Federation, Tajikistan, and Uzbekistan submitted an *International Code of Conduct for Information Security*. In the covering note explaining the proposal, the delegations stated that the rapid development of "information and telecommunication technologies could potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security." It went on to say that the proposed international code of conduct had been elaborated in the form of a potential General Assembly resolution and called for deliberations within the UN framework on this text "with the aim of achieving the earliest possible consensus on international norms and rules guiding the behavior of states in the information space."[13]

By this initiative, China and Russia had adroitly taken advantage of the policy opening provided by the Obama administration's *International Strategy* just a few months earlier. Diplomacy, like nature, abhors a vacuum. The Sino–Russian initiative effectively claimed the diplomatic high ground with a proposed set of norms for responsible state behavior in cyberspace – or "information space," as the Chinese and Russians prefer to term it. That difference in terminology is noteworthy because it reflects a deeper ideological difference in how these governments perceive the issue of cyber security. Western countries tend to consider it as a matter of maintaining an open and secure Internet without constraint on content. China and Russia, in contrast, consider content as a key element of the information space they wish to safeguard.

Although the proposed text did not explicitly address these differences in terminology, they would certainly emerge in any consideration of the proposal. The co-sponsors of this initiative were clever, however, in the form they chose for their set of norms. They presented it as a politically binding code of conduct rather than a legally binding agreement, even though traditionally both China and Russia have advocated legal instruments over political

arrangements. This approach reflected the increased aversion U.S. administrations have shown toward entering into international agreements that require Senate ratification, as opposed to politically binding arrangements undertaken by the executive branch alone such as codes of conduct. Beyond the particular case of the United States, the relative ease of state engagement and the general rapidity to conclude political arrangements have tended to favor them over legal instruments such as treaties in international security affairs (for example, the draft international code of conduct on outer space activities originally presented in 2008 by the European Union,)[14] China and Russia have tailored a proposal that they knew would represent an easier diplomatic "sell" to other states than if they had put forward a draft international treaty.

The Devil Is in the Details

If the form of the proposed code was skillfully designed to appeal to other countries, the content of the code was more problematic and likely to spark controversy. After a rather anodyne preamble, the Sino–Russian Code states its purpose is to identify "the rights and responsibilities of States in information space," echoing the norms of responsible state behavior language set out in the Obama *Strategy*. The core of the code was contained in a set of eleven actions to which states were to voluntarily subscribe. While some of these measures were rather innocuous – with references to bolstering regional cooperation and assisting developing countries to close the digital divide – other actions were decidedly problematic. Three of these actions were especially significant, both for their potential impact on state behavior and for highlighting the challenge in bringing the international community to a common understanding of key norms.

The first such action reads: "Not to use information and communication technologies, including networks, to carry out hostile activities or acts of aggression, pose threats to international peace and security, or proliferate information weapons or related technologies."[15]

The second was couched as a cooperative measure: "To cooperate in combating criminal and terrorist activities that use information and communications technologies, including networks, and in curbing the dissemination of information that incites terrorism, secessionism or extremism, or that undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment."[16]

The third major action was "[t]o reaffirm all the rights and responsibilities of states to protect, in accordance with relevant laws and regulations, their information space and critical information infrastructure from threats, disturbance, attack and sabotage."[17]

It is evident that several of the terms used in these provisions are ambiguous and could be open to widely differing interpretation. Take for example the phrase "hostile activity" in the first measure; hostility is in the eye of the beholder and could include hosting a server which supports the website of an opposition group. Or consider the prohibition on "proliferation of information weapons or related technologies" – beyond the fact that "information weapons" as a category has yet to be defined, what constitutes "proliferation" of these items is also obscure. Would offering online subscriptions to a publication that criticizes state actions qualify as a proliferation of information weapons? Since one could view a cyber attack mounted from someone's laptop as constituting an information weapon, would the ban on proliferation of related technologies extend to marketing these basic computer items? Establishing mutually acceptable definitions of the very equipment or capabilities the code would aim to preclude represents a major hurdle for any future negotiators.

Similarly, the appeal to cooperate in combating criminal and terrorist activities calls for suppressing information that incites "secessionism" or undermines another country's "economic and social stability, as well as their spiritual and cultural environment."[18] It is clear that authorities could interpret almost anything as falling under these categories, and adopting such a measure would provide an authoritarian regime with wide scope for censorship and repression.

Even the superficially benign affirmation of the right of states to protect their "information space" could prove highly problematic in practice. What one state might view as a "disturbance" or even "sabotage" of their information space, another state might simply consider a case of exercising the right to freedom of expression. These examples of inherently problematic features of the text are not to suggest that the problems of a code of conduct for cyberspace are insurmountable or that they render the pursuit of some common ground rules as futile. They do, however, indicate the difficulty in arriving at provisions that would have comparable implications for conduct among states with differing political systems and ideological worldviews.

Moscow and Beijing appear aware that their original proposal might have provoked skepticism (and diplomatic opposition). In January 2015, a revised version of the Code of Conduct was circulated at the UN, one that reflected input received from a series of consultations with other states. In the covering letter, the sponsors declared that their aim was "to push forward the international debate on information security, and help forge an early consensus on this issue."[19] The revised text largely reflects the contents (and concerns) of the original, although there has been a major change on the international security dimension. The ambitious measures to prohibit information weapons and their proliferation have been deleted in favor of a far more general exhortation not "to carry out activities which run counter to the task of maintaining international peace and security."[20]

However, little change has occurred in the measures reaffirming state sovereign rights over Internet policy and practice. The document makes a nod towards human rights by including a reference to the necessity to protect an individual's rights online as well as offline (a formula drawn from an earlier resolution (20/8) of the UN Human Rights Council adopted in July 2012). The revised document does retain a rejection of "interference" in internal affairs and the information control functions relating to the supposed undermining of "stability." For the time being, China and Russia are proceeding cautiously with their initiative, although issuing the revision reflecting some input from others indicates that they are methodically building support for their proposal. The revised version of the Code is formatted like an actual resolution – and China and Russia could submit it for consideration at the UN General Assembly at any time – but the chief sponsors remain rather coy about their ultimate intentions.

The UN Group of Governmental Experts

The measured pace China and Russia are following in building support for their proposed Code may also be tied to a related but distinct UN process currently underway. This is the UN Group of Governmental Experts (GGE) on "Developments in the Field of Information and Telecommunications in the context of International Security," which was established by a widely supported Russian-led General Assembly resolution (66/24) in 2011. The GGE (comprised of representatives of the five permanent members of the UN Security Council and ten other states) met in three one-week sessions in 2012 and 2013, and was successful in producing an agreed-

upon report to the General Assembly for its fall 2013 session. (It is important to note that UN GGEs work on the basis of consensus, thus the report had to be agreed to by all the participating experts.) The GGE had a mandate 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 behavior of States."[21] Given the strong Russian leadership behind the scenes on the GGE, it is not surprising that its orientation was clearly in line with the objectives being promoted in the Sino–Russian draft Code.

The GGE report acknowledged the growth in threats to cyber security and the use of information and communication technologies (ICT) for crime and "the conduct of disruptive activities." The report further recognized that "States also have an interest in preventing conflict arising from the use of ICTs," and warned that "[t]he absence of common understandings on acceptable State behavior with regard to the use of ICTs increases the risk to international peace and security." To avoid these hazards, the report concluded that "international cooperation is essential to reduce risk and enhance security."[22]

The form this international cooperation should take is reflected in the report's sections on norms, confidence-building measures, and capacity building. Under the section on norms, the report affirmed "The application of norms derived from existing international law relevant to the use of ICTs by States is an essential measure to reduce risks to international peace, security and stability."[23] This assertion of the relevance of international law to the new domain of cyberspace was a key objective of the United States and other Western states. They considered it crucial for countries to view the existing international legal framework as compatible with and applicable to cyberspace. At the same time, the applicability of existing international law is immediately conditioned by references to the need for further study on how such norms shall apply to State behavior and the potential for further developing norms. Similarly, the report affirms state sovereignty in the conduct of ICT-related activities and in the state's jurisdiction over ICT infrastructure on its territory. In short, the GGE report did not reconcile the ongoing tensions over the scope of state sovereignty with respect to the Internet.

The role of confidence-building measures as voluntary steps to promote trust among states was another focus of the report. The GGE recommended, "States should consider the

development of practical confidence-building measures to help increase transparency, predictability and cooperation."[24] The report set out an illustrative list of possible measures including exchange of information on national strategies and policies; the creation of bilateral, regional, and multilateral consultative frameworks for confidence building; and enhanced mechanisms for law enforcement cooperation. Although this section presented a useful menu of confidence-building measures, their actual adoption is left up to states for future action.

The report concluded on a modestly upbeat note, declaring that "[p]rogress in international security in the use of ICTs by States will be iterative, with each step building on the last."[25] A more somber outlook might stress that the iterative process may not simply move in the direction of enhanced security, and that state actions can detract from, as well as contribute to, the level of international security in cyberspace. Indeed, the revelations of sophisticated state-conducted actions of cyber espionage and sabotage that emerged around the time of the GGE report's release in 2013 such as the revelations by former NSA contractor Edward Snowden and alleged Chinese attacks on media entities and universities served to underscore the risks to global cyber security if "norms of responsible state behavior" are not developed and implemented.

In order to maintain diplomatic momentum on the issue of cyber security and the role of states, Russia and other sponsors of the GGE process decided to immediately build on the 2013 report by having the General Assembly agree to a further round of GGE study. In its new mode, an expanded GGE of 20 states has been meeting since 2014 and is slated to report by the start of the General Assembly's fall session in 2015. In addition to the existing mandate with its focus on norms of responsible state behavior and confidence-building measures, the GGE is to study "the issues of the use of information and communication technologies in conflicts and how international law applies to the use of information and communication technologies by States."[26] Indications are that these additional aspects are proving more difficult for the new GGE to agree on, and the current GGE may prove unable to produce a substantive report or any report at all. The group's mandate, however, points to the type of specific problems the international community will need to address if it is to ever realize the call for developing general norms.

Critics will also point to the absence of private sector or civil society involvement in elaborating norms. The text of the 2013 GGE report was explicit in saying that states must lead

on developing cyber confidence-building measures, while noting that this work would benefit "from the appropriate involvement of the private sector and civil society."[27] There is little indication that any provision is being made for the current GGE to receive input from civil society or the private sector, and as a result its outcome may lack credibility in certain quarters. Already, civil society is organizing to advocate certain state action. At the fall 2014 session of the UN General Assembly, nine NGOs presented a joint statement calling for states to work to adopt "an effective international legal framework that will prevent cyber attacks and protect the networked infrastructure upon which societies rely for their well-being."[28]

Despite its initial success therefore, it remains to be seen if the UN GGE process can contribute significantly to global norm creation, especially as states begin to articulate differing visions of what constitutes responsible state behavior in cyberspace. Although Russia and China were unable to have the 2013 GGE report go beyond a neutral "taking note" of their proposal for a Code of Conduct, these states will no doubt present the GGE result as validating their current initiative in presenting a set of global norms. Now that they have released a revised version of the Code of Conduct, it is possible that Beijing and Moscow may view the 2015 reporting deadline for the GGE – regardless of its outcome – as the logical point to bring their Code of Conduct proposal forward and seek its adoption by the General Assembly this fall.

Needing a Western Response

Whatever the diplomatic strategy Beijing and Moscow ultimately pursue, it is evident that Western states are reacting warily to the proposed Code. Therefore in the near term, any push for early adoption of the draft Code of Conduct is likely to result in a new East–West divide. The desire to avoid such a divisive outcome explains in large part the restraint its Sino–Russian sponsors have shown. At the same time, the West (in particular its leading nation the United States) having called for the development of a global consensus on norms for responsible state behavior can hardly object when states respond by suggesting a set of norms of their own. Indeed, from the cool reception that some Western capitals have shown the Russian–Chinese proposal, one can discern an irritation that Beijing and Moscow have effectively stolen the

initiative from leading Western powers in presenting a draft set of global norms to the international community.

Instead of simply being miffed over having lost the diplomatic monopoly on norms for responsible state conduct in cyberspace, it would be prudent for Western states to come up with their own version of what these global norms should include. In the competition for intellectual leadership on global norms for cyber security, it is not enough to simply critique China's and Russia's offerings.

Some signs indicate that the United States is starting to articulate what appropriate norms and practical measures include. Officials in the State Department's Office for Cyber Issues have begun in 2014 to call for cooperative measures that would preserve "stability" in cyberspace and remove incentives for attack. These measures would build on practices of state self-restraint, and seek to provide critical civilian information infrastructure with a protective status from cyber attack akin to that that crucial civilian infrastructure currently enjoys under international humanitarian law. There is express interest in pursuing agreement on confidence-building measures "designed to reduce the risk of escalation due to misunderstanding or miscalculation regarding a cyber incident of national security concern…"[29] These are promising initial ideas, but ones which need to be formalized and presented more systematically if they are to represent a coherent set of norms and measures that would constitute an alternative to the Sino–Russian proposed Code of Conduct. Other Western states should also become more engaged in formulating specific standards and practices that are aligned with, and promote the vision of, cyberspace that these states uphold.

A clear Western counter-proposal would also assist those states not enamored with the Sino–Russian text to think through some of the problems inherent in any effort to delineate responsible state behavior in cyberspace. The distinction between offensive and defensive cyber operations in cyber security strategies, for example, will be critical as militaries begin to establish cyber units and develop their capacities. In turn, governments will need to decide on policy limits to inform eventual rules of engagement for their militaries. For example, whether measures to counter cyber attacks would be limited to defensive actions only or whether and under what conditions would offensive cyber operations be authorized. Such internal

deliberations can and should be informed by multilateral debate about whether offensive cyber operations should be permitted in cyberspace, and if so under what constraints. Should one set of rules apply in peacetime and another under conditions of armed conflict that trigger the provisions of international humanitarian law?

Similarly, the difference between computer network attack and computer network exploitation (a crucial demarcation for the military and intelligence establishments respectively) will require serious debate as states may seek to maintain cyber espionage while cooperating to curtail cyber warfare. These examples illustrate the type of thorny policy issues over which even like-minded Western states may differ. It will prove important for detailed consultations on these questions to get underway among allies and partners so that a more coherent cyber security foreign policy can emerge over time. This in turn will serve as a vital precondition for effective diplomatic engagement in forging the envisaged global consensus on norms of state conduct in cyberspace.

Conclusion

The quest for a global consensus on norms of responsible state behavior in cyberspace needs to be purposefully taken up. The international community can ill afford to leave the security of cyberspace to the self-proclaimed ‘cyber warriors.’ The previous official recognition that such norms are desirable requires sustained follow-up. Concerned capitals will have to invest considerable political and diplomatic energy in any effort to forge agreements around such norms. While bilateral consultations and regional arrangements can help, the universal character of cyberspace points to a need for norms that will be global rather than particular in nature. This suggests eventually a dedicated multilateral process under UN auspices.

It is time for states to move from airing broad principles to initiating a more focused diplomatic process to negotiate the content of the new norms. Preserving cyberspace for peaceful purposes on behalf of humanity requires pro-active work to forge some common arrangements to govern state actions. Although states will have to step up to the plate to address this challenge, the private sector as well as civil society, as the chief stakeholders of cyberspace, cannot afford

to be idle on this issue and will need to press their governments to take early and appropriate action if the benign character of cyberspace is to be preserved.

Notes

[1] Ronald J. Deibert, *Black Code: Inside the Battle for Cyberspace* (Toronto: McClelland & Stewart, 2013), p. 88.

[2] *The Cyber Index: International Security Trends and Realities* (Geneva: UN Institute for Disarmament Research, 2013) pp. 1-2, http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf.

[3] Brian Fung, "Cyber Command's exploding budget, in one chart," *The Washington Post*, January 15, 2014, http://www.washingtonpost.com/blogs/the-switch/wp/2014/01/15/cyber-commands-exploding-budget-in-1-chart/.

[4] U.S. Department of Defense, *The Department of Defense Cyber Strategy* (The Pentagon, Washington, DC, April 2015), pp. 6 and 9, http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

[5] *Department of Defense Cyber Strategy*, p. 10.

[6] "PPD 20, U.S. Cyber Operations Policy," Federation of American Scientists, http://fas.org/irp/offdocs/ppd/ppd-20.pdf.

[7] *Ibid.*

[8] For reporting on U.S. government reactions to Chinese cyber intrusions, see: Ellen Nakashima "Confidential Report lists U.S. weapon system designs compromised by Chinese cyberspies," *The Washington Post*, May 28, 2013, http:/www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html; David Alexander "Cyber threats pose 'stealthy, insidious' danger: defense chief," *Reuters*, May 31, 2013, http://www.reuters.com/article/2013/05/31/us-usa-defense-hagel-cyber-idUSBRE94U05Y20130531; Jane Perlez "Hagel, in Remarks directed at China, speaks of Cyberattack Threat," *The New York Times*, June 1, 2013, http://www.nytimes.com/2013/06/02/world/asia/hagel-reassures-asian-allies.html?_r=0.

[9] Megha Rajagopalan, "China suggests U.S. may have fabricated evidence of cyber attacks," *Reuters*, May 29, 2014, http://uk.reuters.com/article/2014/05/29/uk-china-usa-diplomacy-idUKKBN0E914T20140529.

[10] Ting Shi and Michael Riley "China Halts Cybersecurity Cooperation after U.S. spying charges," Bloomberg, May 20, 2014, http://www.bloomberg.com/news/articles/2014-05-20/china-suspends-cybersecurity-cooperation-with-u-s-after-charges.

[11] *Department of Defense Cyber Strategy*, p. 28.

[12] Office of the President of the United States, *International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World* (The White House: Washington, DC, May 2011), pp. 4 and 11, https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

[13] United Nations General Assembly, 66th Sess., (A/66/359), *International Code of Conduct for Information Security*, September 14, 2011, available at: http://cs.brown.edu/courses/csci1800/sources/2012_UN_Russia_and_China_Code_o_Conduct.pdf.

[14] *International Code of Conduct for Outer Space Activities*, version of September 16, 2013, http://eeas.europa.eu/non-proliferation-and-disarmament/pdf/space_code_conduct_draft_vers_16_sept_2013_en.pdf.

[15] *Ibid* p. 4.

[16] *Ibid* p. 4.

[17] *Ibid* p. 4.

[18] *Ibid* p. 4.

[19] United Nations General Assembly, 69th Sess., (A/69/723), *International Code of Conduct for Information Security*, January 13, 2015, available at: https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf.

[20] *Ibid.*

[21] United Nations General Assembly, 67th Sess., (A/RES/67/27), *Developments in the field of information and telecommunications in the context of international security*, December 11, 2012, https://gafc-vote.un.org/UNODA/vote.nsf/91a5e1195dc97a630525656f005b8adf/1432090018b3aa7e85257ad200508ae0/$FILE/A%20RES%2067%2027.pdf.

[22] United Nations General Assembly, 68th Sess., (A/68/98), *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, June 24, 2013, http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98. p. 6-7.

[23] *Ibid* p. 8.

[24] *Ibid* p. 9.

[25] *Ibid* p. 11.

[26] UN General Assembly, 68th Sess., (A/RES/68/243), *Developments in the field of information and telecommunications in the context of international security*, January 9, 2014, http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/243.

[27] *Ibid* p. 10.

[28] "Civil Society statement to First Committee on cyber, disarmament and human security" October 28, 2014, available at www.reachingcriticalwill.org.

[29] U.S. Department of State, "As Prepared Remarks at Georgetown University Institute for Law, Science and Global Security's 2013 International Engagement on Cyber Conference," remarks by Christopher Painter, Coordinator for Cyber Issues at Georgetown University, March 4, 2012, http://www.state.gov/s/cyberissues/releasesandremarks/223075.htm.