Institute for Security & Development Policy

Policy Brief
No. 156 June 19, 2014

Tensions in Cyberspace: Toward a Code of Conduct

Niklas Swanström & Jacob Magnusson

The row between the United States and China, caused by the indictment of five Chinese military officers on account of cyberespionage against private companies in the U.S., illustrates the importance of cooperation and transparency to promote mutual trust. In this regard, efforts should be expended to develop norms and frameworks toward a common code of conduct in cyberspace.

On May 19, the U.S. Department of Justice announced the indictment of five Chinese military officers from the People's Liberation Army on account of computer hacking, economic espionage, and other offenses, against five American corporations and one labor organization. The Chinese government vehemently denied its involvement in any acts of cyberespionage directed against American companies, claiming that the allegations are completely ungrounded.

Last month's indictment has exacerbated tensions between the U.S. and China, undermining other spheres such as trade ties, as well as impeded efforts at building trust in cyberspace. Immediately following the decision, China suspended the activities of the China-U.S. Cyber Working Group, including its next scheduled meeting in July. The Working Group, which was set up in April 2013 to enable the two countries to share perspectives on norms and the application of existing international laws in cyberspace, had held its inaugural meeting in July last year with the participation of high-level civilian and military officials. While the concrete outcomes from the meeting were modest, it had appeared to ease tensions that had arisen from the Snowden leaks, including allegations that the U.S. had spied on Chinese telecoms giant Huawei, among others.

Furthermore, in April, U.S. Secretary of Defense Chuck Hagel had met with Chinese Defense Minister Chang Wanquan to discuss, among other things, a new model of military-to-military relations, including the importance of increased transparency regarding capabilities and intentions in cyberspace. The likelihood of getting such an initiative in place has now decreased significantly, however.

Governing Activities in Cyberspace

The indictment is the first case of charges being brought against a state actor for economic espionage, thus highlighting the delicacy of alleged governmental involvement in illegal activities in cyberspace. The charges principally shed light on worries concerning the increasing costs incurred by different forms of "cybercrime," including, but not limited to, corporate espionage, identity theft, copyright infringement, trade secret theft, and fraud. Indeed, cybercrime is a grave threat to economic security today, by undermining trade, innovation, competitiveness, and economic growth. A joint McAfee-CSIS report released on June 9 estimates the annual cost of cybercrime (including cyberespionage) to the global economy to between $375-575 billion and growing.

The Sino-U.S. case also highlights the problems arising from the lack of consensus on norms for behavior in cyberspace, and its implications are thus significant for cybersecurity in the global context. Chinese officials as well as independent observers have questioned the distinction made by the U.S. government between cyberespionage for national security issues on the one hand and for corporate espionage on the other. In the eyes of the U.S. administration, the former is fair game, while the latter is illegal within international as well as domestic U.S. law. However, because of the lack of consensus on norms guiding behavior in cyberspace, such an assertion is difficult to maintain, as the Chinese reaction clearly shows. The process of rapprochement is made even more difficult by the Chinese concept of "informatization," which takes an integrated approach to military, political, economic, and cultural cybersecurity and according to which cyberespionage for the purpose of

procuring business secrets is indeed part of national security. That the views on the fundamental question of what constitutes cybersecurity differ so radically illustrates the need for dialogue and institutionalized cooperation on the issue.

While there exist international frameworks regulating conduct in cyberspace—the most significant of which is arguably the Council of Europe's Budapest Convention on Cybercrime—they are far from universally embraced. Consecutive Groups of Governmental Experts (GGEs) reporting to the United Nations General Assembly have, furthermore, made some promising progress regarding states' positions on cybersecurity. The most recent GGE, with members from 15 countries, including the permanent members of the UN Security Council, concluded that international law, and in particular the UN Charter, is applicable to cyberspace. However, there is no consensus on *how* precisely international law applies or whether it covers all aspects of cyberspace. A new GGE will hold its first meeting this summer and is scheduled to report to the General Assembly in 2015. These strides notwithstanding, there are still no signs of a comprehensive treaty on the UN level, nor any other universally accepted norms for behavior in cyberspace, which is a considerable shortcoming.

Toward a Code of Conduct

The wider implications of the Sino-U.S. spat calls for action by both governments and international organizations. It is clear that approaches promoting collaboration and development of norms are needed if states are to agree on conduct in cyberspace.

Greater inclusion in present and future dialogues is required. Importantly, the China-U.S. dispute is relevant to other major international actors in pursuit of mutual trust and cooperation in cyberspace—namely the European Union, which would be wise to monitor developments closely considering the EU-China investment negotiations launched in December 2013. The growing presence of cybercrime is by all means a grave threat to economic security that demands action, but a tit-for-tat approach of sanctions and counter-sanctions is not the answer. It is therefore paramount that the approach pursued takes the lack of consensus on norms for behavior in cyberspace into account, while simultaneously protecting national economic interests and private investors. The recently initiated 1.5 track Sino-European Cyber Dialogue, engaging state and non-state experts on cybersecurity, is a step in the right direction in this regard and should be encouraged. However, this process is primarily political and academic, and lacks participation at the operational level, i.e. the military and intelligence community. In order to promote mutual understanding and increased transparency at the political, operational, and corporate levels, it is important that present and future dialogues are inclusion sensitive.

The now-suspended China-U.S. Cyber Working Group should be re-instated and new meetings scheduled. Dialogues of this kind are necessarily long and arduous processes, and several meetings will be needed to create mutual trust. Here, too, it is crucial that the operational level is properly incorporated in the process, so that talks are not limited to the political level. Such inclusion can promote transparency and openness on cyberspace issues, thus strengthening relations. Further, the Working Group should not be confined to discussing cybersecurity in its narrow meaning, but rather take into account the Chinese informatization approach and consider cybersecurity in a broader sense.

Institutionalization in the form of a UN charter is necessary in the long term, and a step-by-step approach should be pursued in the short term. The ad hoc measures of today are not sufficient and could even lead to more tensions. The international community should thus make a joint effort to redress the lack of universally recognized charters governing international norms for behavior in cyberspace. The creation of a proper institutionalized framework would make non-adherence to undertaken commitments more costly and thus less likely. While a comprehensive UN treaty is probably not achievable in the short-term, it should be the desired end goal, since working together toward a common framework is in the self-interest of all parties. To pave the way for such a treaty, governments should take a step-by-step approach, striving for agreement in areas that are less controversial, thereby fostering trust and confidence to discuss more complicated issues. Continuing the work of the UN GGEs, which have had a reasonably positive track record thus far, is one way of getting there. In this context, it is also important that a broader international platform facilitating multilateral discussions on cybersecurity is created. Such a platform could serve to complement bilateral processes, to prevent deadlock in the latter, and in addition can be less sensitive. At a

minimum, governments should pursue an understanding of one another's concerns in the digital sphere, to ensure they come to a common understanding on cybersecurity and to prevent the exacerbation of tensions stemming from a lack of communication.

Dr. Niklas Swanström is Director of ISDP and Jacob Magnusson an intern at the institute.

About ISDP

The Institute for Security and Development Policy is a Stockholm-based independent and non-profit research and policy institute. The Institute is dedicated to expanding understanding of international affairs, particularly the interrelationship between the issue areas of conflict, security and development. The Institute's primary areas of geographic focus are Asia and Europe's neighborhood.

Website: www.isdp.eu