From: SMART Archive
Sent: 6/17/2014 4:21:25 AM
To: SMART Core
Subject: China Uses UN Conference to Promote Its Vision of Cyberspace, Blast U.S. Surveillance

UNCLASSIFIED
SBU

RELEASE IN FULL

REVIEW AUTHORITY: Clarke Ellis, Senior Reviewer

MRN:	14 BEIJING 2134
Date/DTG:	Jun 17, 2014 / 170819Z JUN 14
From:	AMEMBASSY BEIJING
Action:	WASHDC, SECSTATE *IMMEDIATE*
E.O.:	13526
TAGS:	PREL, PGOV, PINR, ECON, KCYB, AINT, TINT, CH
Captions:	SENSITIVE
Subject:	China Uses UN Conference to Promote Its Vision of Cyberspace, Blast U.S. Surveillance

1. (SBU) Summary: During his remarks to open the June 5-6 China-United Nations co-hosted International Workshop on Information and Cybersecurity, PRC Vice Foreign Minister (VFM) Li Baodong delivered a sharp rebuke of U.S. government surveillance while promoting China's vision of peace, state sovereignty, co-governance, and cooperation in cyberspace. China plugged its co-sponsored International Code of Conduct for Information Security, and called for a greater role for the United Nations in Internet governance. Looking ahead to the UN Group of Governmental Experts meeting in July on cyber issues, China called for a discussion of privacy concerns and new international norms in cyberspace to supplement existing international law. Participants were divided over how extensive a role the UN should play in cybersecurity, with most agreeing the UN should continue to facilitate international dialogue on, rather than attempt to manage, cyberspace. End Summary.

China Calls for More Cyber Cooperation...

2. (SBU) China's Ministry of Foreign Affairs (MFA) and the United Nations Regional Center for Peace and Disarmament in Asia and the Pacific (UNRCPD) co-hosted the *International Workshop on Information and Cybersecurity: Towards a Peaceful, Secure, Open and Cooperative Cyberspace* June 5-6 in Beijing. Participants included representatives from ASEAN and P5 member states, Germany, Pakistan, Australia, New Zealand, Japan, Sri Lanka, South Africa, and Chinese and international think tanks. This marked China's first time co-hosting a UN conference on cybersecurity. Panel topics included discussions on states' cyberspace policies and emerging challenges; the formulation of international rules and norms in cyberspace;

the role of the United Nations in promoting cybersecurity dialogue; cyber cooperation among national level actors; and, regional cooperation and capacity building.

...After a Few Opening Barbs

3. (SBU) During his opening remarks, PRC Vice Foreign Minister (VFM) Li Baodong wasted little time in slamming the United States. Without directly naming the United States, Li told participants that the "imbalanced situation" in which "an individual country" could conduct massive surveillance and infringe upon the privacy of other nations' citizens "must be corrected." Li said China was committed to dialogue on cyber issues on the basis of mutual respect, but could not accept a situation in which another country exercises double standards, draws lines out of its selfish interests, defames others, and displays hypocritical, hegemonic behavior. Instead of reflecting on its behavior that has undermined the sovereignty of other nations and the privacy of those nations' citizens, that "individual country" paints itself as a victim.

Panel Highlights: Cyberspace Policies and Emerging Challenges

4. (SBU) During the first session, panelists described aspects of their respective governments' cyber policies and focused on some of the main challenges they face. Sri Lanka Computer Emergency Response Team (CERT) Operations Manager Rohana Palliyaguru described the difficulties ICT (information and communications technology) managers face in convincing their companies' executives to invest in better ICT security systems as the latter group sees no tangible benefits from doing so. Japanese Ambassador for Cyber Policy Shimmi Jun spoke of the need for widespread application of international law in cyberspace and of Japan's short-term plans to provide capacity-building assistance to developing countries in ASEAN, and long-term plans to similarly aid other countries in the Asia-Pacific and Africa. Ambassador Shimmi also strongly endorsed the Budapest Convention on Cybercrime. MFA Cyber Affairs Office Director Li Chijiang said overreliance on another country's ICT products and the unsecure flow of information threatened China's cybersecurity. Countries need laws to manage that flow of information, he asserted.

MFA Cyber Coordinator Outlines PRC Views on Cyber Norms

5. (SBU) Opening the second session on the formulation of international norms in cyberspace, MFA Coordinator for Cyber Affairs Fu Cong echoed many of the same lines -- and requisite U.S.-bashing -- used in VFM Li Baodong's opening address. Fu touted China's role in co-sponsoring the Shanghai Cooperation Organization's (SCO) International Code of Conduct for Information Security (ISCoC) as evidence of China's willingness to make important contributions to international cyber norms-making. The ISCoC had won the support of many countries, he claimed. China was watching with great interest how ICANN (Internet Corporation for Assigned Names and Numbers) would move out from under direct U.S. government control, and believed ICANN should go a step further by physically moving its offices out of the United States so as to be "free of control by unilateral

forces," said Fu. ICANN's government advisory committees (GAC) should have more representatives from developing countries as members, and those members should be given a bigger say in ICANN. Fu also called for strengthening the mandate of the Internet Governance Forum. China was not opposed to the multi-stakeholder model of Internet management, but believed governments should play the primary role.

6. (SBU) Looking ahead to July's meeting of the UN Group of Governmental Experts (GGE), Fu called on GGE participants to study objectively the 2013 GGE report, which he said reflected international consensus to define the principle of sovereignty and the applicability of international law in cyberspace. China believes the body of existing international law is insufficient to deal with the challenges of cyberspace, and that there needed to be new international norms, Fu asserted. The GGE should also discuss states' privacy concerns in the context of norms of behavior in cyberspace. Even though privacy is discussed as part of a broader discussion on human rights at the UN Third Committee, that did not preclude talking about it during the GGE, Fu opined.

7. (SBU) Norms of behavior were also needed to prevent cyber warfare, Fu Cong stressed, adding that the emergence of Stuxnet came against the background of "some countries" developing offensive cyber weapons. It was not acceptable to develop cyber weapons first and seek to control them later, he argued.

8. (SBU) The reason China and other countries so jealously guard the principle of state sovereignty in cyberspace is because "some countries" use the principle of free flow of information to "propagate lies against other governments," explained Fu. Unless countries abide by the principle of non-interference in other states' affairs, China has no choice but to safeguard its sovereignty in cyberspace. The Snowden leaks revealed the magnitude of U.S. surveillance, which made it more than just an "old issue" of state-on-state espionage, argued Fu.

Pushing Back on China's Claims

9. (SBU) Germany's Head of International Cyber Policy Martin Fleischer challenged several of Fu Cong's claims. It was false to assert that a few western countries dominated Internet governance, he said, pointing out that each ICANN member country had one vote in the organization. Fleischer also called it "illogical" to see a link between U.S. oversight over ICANN and NSA surveillance and cast doubt on the view that only under the UN framework could Internet governance be made more democratic and efficient. UK-based International Institute of Security Studies' (IISS) Director of Transnational Threats Nigel Inkster asked rhetorically whether any government that had technical surveillance capabilities on par with those of the U.S. National Security Agency (NSA) would not have used them for national security purposes as the United States had.

Split Over UN Role in Cybersecurity

10. (SBU) In the third session, participants were divided over the role the

United Nations should play in cybersecurity. Representatives from UN agencies described the UN as a unique platform for promoting international dialogue on cybercrime and cybersecurity and building capacity, but dismissed any attempt to outsource cyber issues wholesale to the UN or to ascribe to it the role of global cyber policeman. IISS's Nigel Inkster called for the UN to develop practical working arrangements with entities such as ICANN and the Internet Engineering Task Force (IETF) rather than seeking to supplant them. Chinese Ministry of State Security-affiliated China Institutes of Contemporary International Relations (CICIR) Vice President Yang Mingjie said the UN's inclusiveness and unparalleled authority made it a critical player on cybersecurity issues, and contrasted it with what he called ICANN's lack of inclusiveness. Yang also recommended that the UN ensure it has adequate financial resources to follow up on activities of the Internet Government Forum and the GGE. Georgina Sargison, an official from New Zealand's Ministry of Foreign Affairs and Trade, argued that the UN could not be the main actor on Internet governance issues, and that its main role should instead be as facilitator of such debate.

Challenges and Opportunities of Cyber Cooperation

11. (SBU) During the final two sessions, discussants raised the challenges and opportunities posed by cooperation on cyber issues. MFA-affiliated China Institute of International Studies (CIIS) Associate Research Fellow Xu Longdi reflected his government's view that states must command the central role in guarding cyberspace because only states could "mobilize social forces" and connect policy with technical aspects of cyberspace. U.S. Information Technology Office (USITO) President Matt Roberts stressed that governments alone are ill-equipped to develop Internet standards because they cannot keep up with the pace of innovation. Dialogue and partnership between governments and the private sector are critical to Internet security, he added.

12. (SBU) Republic of Korea Ministry of Foreign Affairs International Security Division Deputy Director Kang Joo-yeon described her country's strategic decision to rely on a free, open cyberspace to drive new economic growth policies. Many countries were losing out on such opportunities by focusing too much on threats, she observed. The 2013 Seoul Conference on Cyberspace increased global awareness of cyber issues and highlighted the need for more cyber cooperation, she recalled, but it was far too premature to entertain talk of any treaty on cyberspace, as some participants had called for. After all, how many countries were even prepared to negotiate a cyberspace treaty when they did not yet fully understand the issues, she asked. Australian Department of Foreign Affairs and Trade Assistant Secretary for International Security Ian Biggs and UK Cabinet Office Assistant Director for Cyber Security and Information Assurance Olivia Preston voiced their governments' support for increasing cyber capacity-building and enhancing cooperation on cyber issues.

The U.S. Viewpoint

13. (SBU) State Department Deputy Coordinator for Cyber Issues Tom Dukes

laid out the U.S. vision for an open, interoperable, secure, and reliable cyberspace. He emphasized the importance of the free flow of information and U.S. support for the multi-stakeholder system of Internet governance. Dukes noted the U.S. participation in Brazil's recently concluded Net Mundial conference, and cited U.S. support for the upcoming UN GGE and the development of cyber confidence-building measures in fora such as the Organization for Security and Cooperation in Europe. Finally, he pointed out that the SCO ISCoC is fundamentally at odds with freedom and human rights, and emphasized the importance of bilateral and multilateral dialogue on cyber issues.

Signature:	KRITENBRINK
Drafted By:	BEIJING:Flens, William (Bill) (Beijing)
Cleared By:	SCCI: TDukes ECON: THilleary ECON: KWald
Approved By:	POL:Heller, James R (Beijing)
Released By:	BEIJING:Flens, William (Bill) (Beijing)
Info:	BEIJING, AMEMBASSY *ROUTINE* ; CD GENEVA, USMISSION *ROUTINE* ; WHITE HOUSE NATIONAL SECURITY COUNCIL WASHINGTON DC *ROUTINE* ; SECDEF WASHINGTON DC *ROUTINE* ; CIA WASHINGTON DC *ROUTINE* ; DIA WASHINGTON DC *ROUTINE* ; HQ USPACOM *ROUTINE* ; ASEAN REGIONAL FORUM COLLECTIVE *ROUTINE* ; UN SECURITY COUNCIL COLLECTIVE *ROUTINE*
Dissemination Rule:	Archive Copy

UNCLASSIFIED
SBU