S. RAJARATNAM SCHOOL
OF INTERNATIONAL STUDIES
A Graduate School of Nanyang Technological University

RSIS COMMENTARIES

No. 046/2013 dated 18 March 2013

US-China Cyber Talks:
Internet Security in the Global Economy

By C. Raja Mohan

Synopsis

A series of recent statements from Washington and Beijing suggest the US and China may be preparing for an important dialogue on cyber security. Focused on the economic implications of cyber espionage, the incipient Sino-US dialogue could define the terms of the global debate on developing cyber norms.

Commentary

THE US national security adviser Tom Donilon this month pointed to the unacceptable frequency and intensity of Chinese cyber attacks on American corporations and called for a comprehensive dialogue with Beijing. Until now the global debate on cyber security has been centered on the challenges of controlling Internet crime, coping with hostile attacks on critical infrastructure like electricity grids, and developing legal norms to limit cyber conflicts among nations.

Donilon's remarks at the Asia Society in New York helped draw international attention to the impact of cyber warfare on the global economy and the future of US-China commercial ties. Donilon urged Beijing to recognise the dangers that the cyber theft of American intellectual property poses to the stability of the global economy; investigate and put an end to these attacks; and start negotiations on drafting a code of conduct.

Commercial or military espionage?

A few days before Donilon spoke, the US cyber security firm Mandiant published a report which traced most of the cyber attacks on the US corporations to a secret Chinese military unit, numbered 61398, located in a 12-storey building in Shanghai. That corporations spy on each other within and across nations is not new. It is the Chinese military's decision to deploy massive cyber resources against the US companies that is startling.

The PLA's objective is widely seen as part of an effort to alter the strategic balance between China and the US by narrowing the gap between the two countries in the high technology sector.

China's massive cyber efforts have begun to blur the distinction between commercial espionage and national security and the Obama Administration is eager to work out a set of mutually-acceptable constraints. This outreach to Beijing complements Obama's determination to defend the US economy, critical national infrastructure and American corporations against cyber attacks originating from China and other external sources. Obama also met in mid-March with the CEOs of thirteen major US corporations to discuss collaboration between the government and business on strengthening America's cyber security.

Obama-Xi phone chat

Officials and media commentators in Beijing, however, say the US is unfairly targeting China. They say China is also a major victim of cyber attacks and insist that most of those originate from the US. They call for an end to "irresponsible criticism" of China and jointly develop rules of the road for international cooperation in cyber space.

The question of cyber security in the economic realm also came up in the phone conversation between Obama and the Chinese leader Xi Jinping after he was formally elected as the President of China. Xi apparently agreed to start talks with the US on cyber security and the new prime minister Li Keqiang publicly affirmed China's interest in building a peaceful relationship with America in his first press conference on the margins of the National Peoples' Congress.

Cyber security, then, could be at the top of the agenda in the American and Chinese quest for a 'new type of relationship' between a rising China and the dominant power of the international system. The US Treasury Secretary Jack Lew who is scheduled to visit China this week is expected to probe the Chinese leaders for the terms of the bilateral dialogue on cyber security.

Washington's new tone of avoiding a confrontation with China came through in Donilon's remarks at the Asia Society: He said: "Economies as large as the United States and China have a tremendous shared stake in ensuring that the Internet remains open, interoperable, secure, reliable, and stable. Both countries face risks when it comes to protecting personal data and communications, financial transactions, critical infrastructure, or the intellectual property and trade secrets that are so vital to innovation and economic growth."

New global discourse on cyber security?

Despite the many tensions in the bilateral relationship, the Chinese public reaction to the spate of recent US allegations on cyber theft and commercial espionage has been moderate. There have been substantive Track Two conversations between the US and China on the economic dimension of cyber warfare and the need for building mutual trust.

The incipient Sino-US bilateral dialogue has the potential to alter the current international discourse on cyber security. Until now Russia has led the debate in multilateral forums like the United Nations on information security. Russia, China and many developing countries have also ranged themselves against the US and the West on questions relating to Internet freedom and the sovereign right of the states to regulate and control the cyber space.

Although these ideological issues will have some salience, the new Sino-US dialogue is about managing the profound interdependence between the world's two largest economies in the cyber age.

Just as the US and the Soviet Union defined the nuclear discourse last century, Washington and Beijing are likely to shape the international regulation of the cyber domain in the coming decades. Once there is a bilateral agreement between America and China on a basic set of norms, it could provide the nucleus for a broader multilateral regime for cyber security.

C. Raja Mohan heads the strategic studies programme at the Observer Research Foundation, Delhi and is adjunct professor at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University in Singapore.