'Cybersecurity'
Threat or Opportunity

Saikat Datta
Policy Director
Centre for Internet & Society,
India

2nd China-India Think Tank Forum
Beijing, 24-25 June 2017

THE CENTRE FOR internet & society

'Themes'

Voices from the 2nd China-India Think Tank Forum

'Made in China 2025...will have two approaches – industrialisation & Information Technology...intelligent manufacture & new generation of IT'

- Prof Huamg Qunhui

DG, Institute of Industrial Economics

'We need to move from de-globalisation to re-globalisation'

- Prof Li Xiangyang

DG, National Institute of International Strategy

'Failure of Strategic Communication leads to mismatch of goals and becomes confrontational. We need a new security architecture'

Prof Madhu Bhalla,

Editor, India Quarterly, ICWA

'Cybersecurity'
~
Threat or Opportunity

- A threat & an opportunity to global stability
- Blurs the State & Non State Actor
- Needs a New Global Security Architecture
- Serves as the pivot to new and intelligent industrialisation
- Is the Key To Transitioning From De-globalisation to Re-gobalisation

'China's Plan of Action in International Strategy of Cooperation on Cyberspace'

- Peace & stability
- Rule based order in Cyberspace
- Partnership in Cyberspace
- Reform of Global Internet Governance System
- International Cooperation on
  Cyber Terrorism & Cyber Crimes
- Protection of Citizens' Rights & Interests Including
  Privacy
- Digital Economy & Sharing
  of Digital Dividends
- Global Information Infrastructure Development and

'India's National Cyber Policy'

- Secure Cyber system environment
- Assurance framework for the
- Regulatory framework
- Protection of Resilience of Critical Information Infrastructure
- Fiscal benefits to businesses that adopt best practices
- Global best practices in information security, risk management, business continuity management and cyber crisis management
- Harmonisation of international regulatory frameworks

`Budapest Convention *on* Cyber Crimes'

'China'

- China's refusal to accede to the Budapest Convention on Cyber Crime reflects its developing state-centric approach to international agreements on cyberspace. The Convention is a multilateral agreement that serves as a framework for international cooperation on cyber crime and a guide for the development of national cyber crime legislation

- In Track II discussions in 2012 between the U.S. think tank Center for Strategic and International Studies (CSIS)

- China's Institutes of Contemporary International Relations (CICIR), CICIR opined a UN treaty could be better at addressing the needs of developing countries in fighting cyber crime than does the Council of Europe-developed Convention.

- CICIR was also concerned that Convention provisions on transnational evidence collection for prosecutions of cyber crimes could violate state sovereignty

'India'

- India has refused to accede to the Budapest Convention on Cyber Crime

- India has argued for a new convention that is far more participatory and addresses concerns of developing countries

- India believes that any new convention or agreement on a global common such as the internet needs new statutory frameworks

- India is concerned that the Convention's provisions on transnational evidence collection for prosecutions of cyber crimes could violate state sovereignty

- India has insisted that a new Convention is drafted with active participation and consultation of new member states

'Wassenaar Arrangement'

- India & China are not members of the Wassenaar Arrangement.

- China and the Wassenaar Arrangement held 5 rounds of dialogues between April 2004 & November 2008

- During the talks, the two sides exchanged in depth views on issues in the field of the export control for conventional arms and dual-use goods and technologies

- India has been making a bid to join four multilateral export control regimes; the NSG, the Missile Technology Control Regime (MTCR), the Wassenaar Arrangement, and the Australia Group.

- India's export controls are in line with the Wassenaar Arrangement

'Bilateral Insecurities'

- Hostage to mutual suspicions – 'failure of strategic communication'

- Competitive neighbours

- Unsettled borders

- China, Pakistan & state-sponsored terrorism

- Tibet & The Dalai Lama

- Reshaping the Global Order – Differing versions of Re-globalisation

'Bilateral Co-operation'

- India has bilateral cyber dialogues with 11 countries

- India has recently obtained the necessary internal approvals for initiating a cyber dialogue with China

- The decision to initiate a bilateral cyber dialogue comes in the background of the interest expressed by China during the 5th meeting of the India-China JWG on CT in March 2012 to have a comprehensive dialogue on Cyber issues.

- This proposal was repeated by the Chinese side to the Indian Expert on the sidelines of the UNGGE Meeting in June 2013\

- Both India and China have been actively participating in various international fora such as the United Nations Group of Governmental Experts (UNGGE), ASEAN, UNODC, BRICS and SCO which are deliberating on various cyber issues such as the applicability of International Law and Norms of responsible

'SALT *to* START'

Learnings from the Strategic Arms Reduction Talks (SALT) to the success of Strategic Arms Reduction Treaties (START)

- Premised on the doctrine of Mutually Assured Destruction (MAD)

- Transparency of military posture

- Confidence Building Measures (CBMs)

- From Suspicion to Cooperation

'Recommendations *for* Areas of Cooperation'

- Mutual Legal Assistance Treaty (MLAT) on cyber issues

- Joint Information Sharing & Analysis Centre for Cyber Incidents

- Research on Cryptography

- Build Capacity on Critical Information Infrastructure Centre

- Emphasis on FinTech & Internet of Things (IoT)

- Joint Expert Group on Reforming Wassenaar Arrangement, Budapest Convention & Talin Manual 2.0

'Thank You'