Celebrating 50 Years of Objective Research

idsa
INSTITUTE FOR DEFENCE STUDIES & ANALYSES
रक्षा अध्ययन एवं विश्लेषण संस्थान

18th asian security conference 2016

Securing Cyberspace: Asian and International Perspectives

February 9-11, 2016

asc
asian security conference 2016
Securing Cyberspace: Asian and International Perspectives

CONFERENCE
BOOKLET

asian
security
conference
2016

18th Asian Security Conference

Securing Cyberspace: Asian and International Perspectives

(February 9-11, 2016)

Organised by

idsa
INSTITUTE FOR DEFENCE
STUDIES & ANALYSES
रक्षा अध्ययन एवं विश्लेषण संस्थान

Contents

About IDSA

The Institute for Defence Studies and Analyses (IDSA) is a non-partisan, autonomous body dedicated to objective research and policy relevant studies on all aspects of defence and security. Since its inception, IDSA has served as a forum to debate important aspects of national and international security. Its mission is to promote national and international security through the generation and dissemination of knowledge on defence and security-related issues.

IDSA was established as a registered society in New Delhi on November 11, 1965. The initiative for setting up the Institute came from then Defence Minister Shri Yeshwantrao Chavan, who was one of the Institute's founding members. Over the last forty-plus years, IDSA has played a crucial role in shaping India's foreign and security policies, including with respect to nuclear weapons, military expenditure, and conventional and non-conventional threats to India.

IDSA has a well-qualified multi-disciplinary research faculty drawn from academia, defence forces and the civil services, and which represent a diversity of views. Research at the Institute is driven by a comprehensive agenda and by the need to provide impartial analyses and policy recommendations. IDSA's journals, monographs, briefs, and books are the principal mediums through which these analyses and policy recommendations are disseminated.

The IDSA website offers in depth insight into the working of the Institute with a user friendly interface. Regular updates on the events at IDSA can be found in the Media Briefs and IDSA News pages.

Research Centres

- East Asia
- West Asia
- South Asia
- Military Affairs
- North America
- Internal Security
- Europe & Eurasia
- Strategic Technologies
- Non-Traditional Security
- Nuclear and Arms Control
- Southeast Asia and Oceania
- Defence Economics & Industry
- Africa, Latin America, Caribbean & UN

ABOUT ASIAN SECURITY CONFERENCE

The Asian Security Conference (ASC) is a major calendar event of the Institute for Defence Studies and Analyses (IDSA), New Delhi which is organized in early spring each year. Since 1999 when the conference was first held, it has become an important forum for debating issues relating to Asian Security. The ASC provides an opportunity for policy makers, scholars and security analysts, both from India and abroad, to share their views on the security challenges facing the continent.

The contemporary strategic context is increasingly defined by the rapid growth of major Asian economies and the rapidly increasing interest the major powers are evincing in the region. It has also resulted in a perceptible shift in power to the Asian continent. While the emerging power shift is full of promise and opportunities, there are important concerns that cannot be ignored. Asia's statesmen face a variety of challenges, which, if ignored or viewed with less concern, could lead to further instability and insecurity in the region. In this backdrop the ASC looks at various emerging trends and changes in the Asian security context and forms a platform for discussion and debate. The ASC serves as the best available vehicle in the Asian region for developing and channeling astute and effective public policy on defence and security. It can also be regarded as an important academic platform for scholars to discuss new ideas and theories.

Previous Asian Security Conference (ASC)

2015: Asian Security: Comprehending the Indian Approach

2014: Emerging Strategic Trends in Asia and India's Response

2013: Emerging Trends in West Asia: Regional and Global Implications

2012: Non-Traditional Security Challenges- Today and Tomorrow

2011: Towards A New Asian Order

2010: Asian Strategic Futures 2030 : Trends, Scenarios and Alternatives

2009: The Changing Face of Conflict and Evolving Strategies in Asia

2008: Asian Security in the 21st Century

2007: Evolving Security Dynamics in Southeast Asia – Emerging Threats and Responses

2006: Changing Security Dynamic in West Asia: Relevance for the Post 9-11 Systemic

2005: Changing Security Dynamic in Eastern Asia: Focus on Japan

2004: United Nations, Multilateralism and International Security

2003: Asian Security and China in the Period 2000-2010

2002: Asian Security Strategies in a Period of Uncertainty

2001: Reshaping Asian Security

2000: Asia’s New Dawn the Challenges to Peace and Security

1999: Asian Security in the 21st Century

Concept Note

Securing Cyberspace: Asian and International Perspectives

Cybersecurity is increasingly drawing attention from policy makers as the world becomes increasingly interlinked and dependent on digital pathways. Use of cyber space by governments, businesses and individuals has provided economic benefits and helped connect the world in beneficial ways. Simultaneously, however, there are attempts being made by state and non-state actors to deny its legitimate use by others. Use of cyber space for espionage, both commercial and security-related, are common. Its use by criminals and extremists is no less dangerous. Managing this nascent and rapidly developing threat has proved to be problematic given that it now touches almost every aspect of human existence, from communication to commerce. It equally impact on a variety of stakeholders, individuals, corporations and states, all with differing priorities and perspectives. The large number of users and actors involved, and their varying perceptions of the threats and responses to emanating from cyber space have led to conflicting voices on how best to mitigate and overcome them.

Even as the connected systems and networks have grown more intertwined and complex, Cyberspace is being used for a variety of malicious activities, from crime to state-sponsored attacks on critical infrastructure. The interconnectedness of cyber networks means that even the most basic responses end up having a ripple effect or unintended consequences. Maintaining a balance between security and benefitting from the many opportunities provided by the deployment of new cyber technologies is proving to be one of the most vexatious issues of the 21st century.

The risk from cyber threats to government agencies, private enterprises, public sector undertakings and research institutions of strategic importance can manifest in many forms. A Distributed Denial of Service (DDoS) attack can disrupt business operations or it may cause severe outages, thereby having a direct impact on their revenue and reputation. Companies also face the risk of losing trade secrets or intellectual property rights. Moreover, a massive data breach for companies or governance portals storing data of customers or citizens can compromise personal information. A cyber-attack on entities that are part of critical infrastructure can have a debilitating impact on national security. The risk increases manifold for electricity grids, nuclear installations, and telemetry/command and control network of space assets. Surprisingly, social media, as a threat vector, has become a channel of least resistance for threat actors to conduct reconnaissance, identity thefts and gather information on employees, projects, systems and infrastructure, besides spreading hateful propaganda and enticing impressionable youth to follow extremist ideologies.

Cyberspace has become an intricate constituent of national power. The strategies for the development of Cyberspace are not just restricted to civilian purposes; rather, this domain now falls well under the ambit of the armed forces. With the advent of Network Centricity in military operations and Revolution in Military Affairs, armed forces are at elevated risk of cyber incidents. The integrated use of land, air, maritime and space assets for enhanced domain awareness or real-time information access warrants the armed forces to build expertise in both defensive and offensive cyber operations. Nation states have documented their Cyber Strategies and executed them in the form of Cyber Commands, both overt and covert. With the military dimension, Cyberspace is witnessing a race for development and deployment of cyber weapons. An arms control regime, the Wassenaar Arrangement has enlarged its controls list in consonance with the way Cyberspace has altered present day security landscape. The development of cyber weapons and their potential usage against high value targets has been one of the major security concerns for nation states.

The threats in Cyberspace are varying in nature and intensity. Leading companies operating in the domains of energy, telecommunications, finance, and transportation sectors are targets of Advanced Persistent Threats (APT).

Non-state actors, such as terrorist organizations and criminal syndicates have become tech-savvy, thereby employing human resources to develop malware. These tools are used extensively in committing Cybercrime. Terrorist organizations leverage the benefits of Cyberspace, harnessing it for ideology propagation, recruitment and communication. The terrorist organization, the Islamic State in Iraq and Syria (ISIS) has been a prime case study. It has tremendous presence on social media helps spread its propaganda and recruit sympathizers across the globe. Al-Qaeda is also reported to have developed encryption software to secure their communication in Cyberspace.

As the extent of commerce transacted over Cyberspace grows, along with increasing reliance on information technology to drive cost-efficiencies, the risk exposure to enterprises have increased. According to the 2013 Security Threat Report published by the cyber security company, Sophos, Asia accounted for eight of the top-10 countries most vulnerable to Cybercrime. Asia, the largest continent on earth, represents 60 percent of the world's population. It is the fastest growing economic region globally. On the other hand, the unprecedented growth of rising economies, rapid industrialisation, rising demand for energy, expanding markets and, depleting natural resources have led to competition and confrontation with respect to the access and control of resources. As Asia continues to grow its share of the global trade and commerce, the threats from cyber-attacks are expected to increase in tandem.

Cyber-attacks, like many of the new security challenges, are transnational in origin and nature, and no nation can combat them alone. Despite variations in ethnic, economic and government systems, Asian countries need robust security architecture to resolve the issues specific to the geographical region as well as international issues detrimental to Asia's economic and societal growth.

With the shift of power towards Asia, its representation in the rule-making mechanisms and inputs towards creating a secure cyberspace is critical to international politics, the world economy, and the credibility of international institutions and cybersecurity regimes. Within Asia, cyber threats have altered the security perceptions of institutions and government systems. Against this backdrop, the Institute for Defence Studies and Analyses, New Delhi will organise the 18th Asian Security Conference focusing on the emerging threats and challenges from cyber domain to national and regional security. The two-and-a-half-day conference will consider international and regional responses to cyber security and the scope for cooperation amidst varying national policy frameworks and legislations.

The major themes to be discussed include the following:

Day One

Session 1: The Global Cybersecurity Environment

Session 2: International and Regional Responses to issues in Cybersecurity

Session 3: Non-State Actors and Cyberspace

Day Two

Session 4: Securing Strategic Critical Infrastructure

Session 5: Cybersecurity and the Digital Economy

Session 6: Role of Military in Cybersecurity

Day Three

Session 7: Cybersecurity Futures

CONFERENCE PROGRAMME

DAY 1: Tuesday, February 9, 2016

09:15-09:40	Registration
09:45-10:15	**Inaugural Address**
Welcome Remarks:	Shri Jayant Prasad, Director General, IDSA
Key Note Address:	Air Marshal PP Reddy VM, ADC, Chief of Integrated Defence Staff
Vote of Thanks:	Brig. Rumel Dahiya (Retd), Deputy Director General, IDSA
10:15-10:45	Tea
10:45-13:00	**Session 1 - The Global Cybersecurity Environment**
Chairperson:	Nitin Desai
Ammar Jaffri	Cyber Security Challenges & Opportunities in the Fast Changing World Today
Varun Sahni	Cyber Redefinitions and the Challenged State: Security Implications
Greg Austin	Mutual Restraint in the Cyberspace Diplomacy of Great Powers
Cuihong Cai	Global Cybersecurity Environment: Perspectives of the US and China in Comparison
Yasuaki Hashimoto	Present Situation of Japanese Cyber Security
13:00-14:00	Lunch
14:00-15:30	**Session 2 - International and Regional Responses to Cybersecurity Challenges**
Chairperson:	Latha Reddy

Alexandra Kulikova	Working out the Rules of Global Cyberspace Governance
Nandkumar Saravade	International and Regional Responses to Cybersecurity Challenges
Candice Tran Dai	Economic Dimensions of National Cybersecurity Strategies in the Asia-Pacific Region
Munish Sharma & Cherian Samuel	A South Asian Regional Cybersecurity Cooperation (SARCC) Forum: Prospects and Challenges
15:30-16:00	Tea
16:00-17:30	**Session 3 - Non-State Actors and Cyberspace**
Chairperson:	Ravi Kant
Alok Vijayant	Asymmetrism in Cyberspace: State vs. Non-state Actors
Sanjeev Relia	Non-State Actors and Cyberspace: An Overview
Arun Mohan Sukumar	State and Non-State: Residual Actors in Cyberspace
Gillane Allam	Non-State Actors & Cyberspace- A North African Perspective

DAY 2: Wednesday, February 10, 2016

10:00-11:00	Keynote Address by Arvind Gupta, Deputy National Security Advisor
11:00-11:30	Tea
11:30-13:00	**Session 4 - Securing Strategic Critical Infrastructure**
Chairperson:	Alhad G. Apte
Ted Lewis	Challenges of Cybersecurity: Malware and AS-level Structure

Kah-Kin Ho	Evolving Role of Government in Critical Infrastructure Protection
Jana Robinson	Governance Challenges at the Intersection of Space and Cybersecurity
Caroline Baylon	Cyber Security Threats to Critical Infrastructure: A Case Study of Nuclear Facilities
A. Vinod Kumar	Securing Critical Infrastructure from Cyber Threats: Developing Defence, Deterrence and Norms
13:00-14:00	Lunch
14:00-15:30	**Session 5 - Cybersecurity and the Digital Economy**
Chairperson:	V. K. Saraswat
Liam Nevill	Challenging Opportunities for Asia-Pacific's Digital Economy
Madan M. Oberoi	New Technologies and New Forms of Crime: Need to Recalibrate Law Enforcement Strategy / Procedures / Law
IL Seok, OH	Korean Legal Initiatives to combat Cybercrime and enhance Digital Economy
Uchenna Jerome Orji	Regionalising Cybersecurity Governance in Africa: An Assessment of Responses
15:30-16:00	Tea
16:00-17:30	**Session 6 - Role of Military in Cybersecurity**
Chairperson:	Prakash Menon
Liina Areng	Role of Military in Cybersecurity
Amit Sharma	The Triad Theory of Cyber Warfare: A Framework for Strategic Cyber Warfare

Caitriona Heinl	International Military Cyber Cooperation in Asia
Li-Chung Yuan	Role of Military in Cyberspace: Case of Republic of China (Taiwan)

DAY 3: Thursday, February 11, 2016

10:00-11:30	**Session 7 - Cybersecurity Futures**
Chairperson:	K. Santhanam
Tobby Simon	Cybersecurity Futures
Sico van der Meer	Defence, Deterrence, and Diplomacy: Foreign Policy Instruments to Increase Future Cybersecurity
John Ellis	Disruptive Technologies and the Trusted Cyber Future
Jonathan Reiber	Cybersecurity Futures and the US-India Strategic Partnership
11:30-12:00	Tea
12:00-14:00	**Session 8 - Panel Discussion on Way Forward**
Chairperson:	Gulshan Rai
	Ammar Jaffri
	Gillane Allam
	Greg Austin
	Kiran Karnik
	N Balakrishnan
	Santosh Jha
Vote of Thanks	
14:00-15:00	Lunch

Profiles of Participants

&

Abstracts

Key Note Address

Air Marshal PP Reddy, VM, ADC

Chief of Integrated Defence Staff

Air Marshal PP Reddy, VM took over as Chief of Integrated Defence Staff to the Chairman Chiefs of Staff Committee on 01 Jul 14. He was commissioned as a Fighter Pilot in the Indian Air Force in Jun 1977. He is an alumnus of Rashtriya Indian Military College, National Defence Academy and Defence Services Staff College, Wellington.

He is a Qualified Flying Instructor and an Experimental Test Pilot who has flown 3600 hrs on various types of fighter as well as transport aircraft, including SU-30 MKI. He has commanded a MiG-27 Squadron and a Fighter Base in Kashmir Valley. He has worked in the Plans Branch at Air HQ and was instrumental in the implementation of SU-30 MKI, IL-78 Flight Refueller Aircraft and MiG-27 upgrade programs. He has also served as the Chief Test Pilot at Aircraft and Systems Testing Establishment, Air Adviser at High Commission of India, London, Senior Officer-in-Charge Administration at South Western Air Command and Senior Air Staff Officer at Training Command. He was the Director General (Inspection & Safety) at Air HQ prior to his present appointment.

He is decorated with the Presidental Award, ‘Vayusena Medal’.

Welcome Address

Jayant Prasad

Director General
Institute for Defence Studies and
Analyses, New Delhi

Shri Jayant Prasad is Director General, Institute for Defence Studies and Analyses, New Delhi. He was India's Ambassador to Afghanistan, Algeria, Nepal, and the UN Conference on Disarmament, Geneva. At headquarters, in the Ministry of External Affairs, he served as Special Secretary (Public Diplomacy), and Head of the Americas and the Multilateral Economic Relations Divisions. He was Rapporteur of the U.N. Commission on Human Rights, Geneva (1986-87), Fellow at the Weatherhead Center for International Affairs, Harvard University (1998-99), member of U.N. Secretary-General's Advisory Board on Disarmament Matters (2005-07), and Visiting Scholar, Center for the Advanced Study of India, University of Pennsylvania (2014-15). Before his 37-year public service career, he was lecturer in history, St. Stephen's College, University of Delhi, after completing his studies at Modern School, St. Stephen's College, and Jawarharlal Nehru University.

Vote of Thanks

Rumel Dahiya

Deputy Director General
Institute for Defence Studies and
Analyses, New Delhi

Brig Rumel Dahiya, SM (Retd) is Deputy Director General at the Institute of Defence Studies & Analyses. He is also Coordinator of the Military Affairs Centre and Managing Editor of the Journal of Defence Studies.

Brig Dahiya is an Indian Army veteran with extensive command and staff experience spanning 32 years, including in counter-insurgency operations. He previously served as a Defence Attache to Turkey, Syria and Lebanon, and with the Indian Military Training Team in Bhutan. He also served with Military Operations Directorate of the Indian Army and Net Assessment Directorate at Integrated Defence Staff. Brig. Dahiya is a graduate of the National Defence College and Defence Services Staff College. He was awarded the Sword of Honour and Gold Medal at the Indian Military Academy at his commissioning.

Session 1

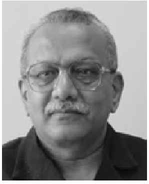
The Global Cybersecurity Environment

Tuesday, February 9, 2016

1045h - 1300h

Chairperson

NITIN DESAI



Shri Nitin Desai was formerly the Chief Economic Adviser in the Ministry of Finance, Government of India and later Under Secretary General of the UN and Chair of the Multi-stake holder Advisory Group that organises the annual UN Internet Governance Forum. He was also the Chairman of the IDSA Task Force on Cyber Security.

AMMAR JAFFRI

Ammar Jaffri is President of Pakistan Information Security Association. He has over 40 years of experience in Governance, Digital Forensics, Information Technology, Security, Education and Philanthropy. He has served and led different departments in the Federal Government of Pakistan, and has been recognized with some of the highest industry honors in Pakistan as well as internationally.

He serves as the Pakistan point of contact for a number of international initiatives on Cyber Security like the Microsoft Law Enforcement Forum, G-8 24/7 High Tech Crime Network, the OIC-CERT, SAARC CERT, APCERT, Council of the European Union, and with INTERPOL. He retired as the Additional Director General of the Federal Investigation Agency of Pakistan in 2010, and is currently engaged in various public and private projects in a private capacity. He is a well-known speaker on a wide range of subjects including Information Security, Electronic Governance, Business Continuity Planning, Electronic Banking, and emerging trends in communication.

Cyber Security Challenges & Opportunities in the Fast Changing World Today

Ammar Jaffri

The paper deals on the following aspects.

i) Use of Cyberspace in Asian Countries.. Future trends and opportunities.

ii) Use of Cyberspace by Criminals & terrorist organizations.

iii) How to remain secure in cyberspace..... Challenges and Solutions.

iv) Need for regional cooperation for securing the Cyberspace.

v) Use of Internet in Development Sector (Health, Education,etc)

vi) Need for regional cooperation (E-SAARC as a Case study)

Varun Sahni

Varun Sahni is Professor in International Politics at Jawaharlal Nehru University, New Delhi. He edits International Studies and South Asian Survey and speaks annually (since 2006) at the National Defence College (NDC) and several times a year (since 1997) at the Foreign Service Institute, New Delhi. He has been a Jury Member of the Jawaharlal Nehru Award for International Understanding. An Inlaks Scholar, he wrote his doctoral dissertation on the political role of the Argentine Navy at the University of Oxford (1991). He has written 105 research articles on nuclear deterrence issues, regional security, emerging balances in the Asia-Pacific, evolving security concepts, emerging powers, international relations theory and Latin American issues. He has been visiting professor at important universities in Mexico City, Washington, DC and Canberra. For his “outstanding contribution to research and teaching”, he was conferred the V.K.R.V. Rao Prize in Social Sciences for 2006 by the Indian Council of Social Science Research. From December 2008 to January 2012, he served as the 10th Vice-Chancellor of the University of Jammu.

Cyber Redefinitions and the Challenged State: Security Implications

Varun Sahni

States are static because they are rooted in territory. World politics, on the other hand, is increasingly dynamic, consisting of networks and flows rather than actors. Information technology (IT), i.e. technology relating to the production, manipulation, storage, communication and dissemination of information, is redefining human and social possibilities, thereby posing some fundamental challenges to the sovereign territorial state. The first redefinition pertains to people: cyberspace is creating novel human aggregations and social configurations and throwing up new possibilities of community. The second challenge is spatial and relates to the new coordinates of location that self-evidently exist in cyberspace. A concrete sense of place emerges out of the specific meanings that individual human beings and social collectivities ascribe to empty, abstract space; cyberspace radically transforms both by offering alternate places and parallel spaces. The third challenge is about the purposes and manifestations of power: cyberspace simultaneously augments the capabilities of government but also magnifies the demands and expectations placed by civil society upon it, besides providing insurgents with new ways to challenge established power structures. Fourthly, cyberspace fundamentally challenges notions of exclusive jurisdiction that are inherent to traditional understandings of statehood. Perhaps it is not coincidental that the challenges emanating from cyber redefinition impact upon the four classical elements of statehood - population, territory, government and sovereignty - and have a significant impact upon state security. Challenges not adequately addressed and dealt with become existential threats. As states, societies and economies become ever more dependent upon IT, cyberspace will inevitably become a theatre of war.

Greg Austin

Greg Austin is a Professorial Fellow with the EastWest Institute in New York and a Professor at the Australian Centre for Cyber Security at the University of New South Wales, Canberra, at the Australian Defence Force Academy. He is the author of several highly reviewed books on international security, especially on Asia. His latest book is *Cyber Policy in China* (Cambridge: policy 2014).

Mutual Restraint in the Cyberspace Diplomacy of Great Powers

Greg Austin

There has been a strong tension in the cyberspace diplomacy of the great powers between the impulse to collaborate for common interests and the countervailing persistence of divergent national military and security needs. Both tendencies saw important evolutions in 2015. New agreements for cooperative efforts and mutual restraint were reached in several forums, such as the G20 and the United Nations Group of Governmental Experts. At the same time, several states published new plans or made new announcements about stepping up military and national security-related activity in cyberspace in ways that suggested an escalating cyber arms race. The middle ground between these two impulses was occupied by new uncertainties in interstate relations about technology transfer between states in the ICT sector. The paper sketches this recent evolution in cyberspace diplomacy with a special focus on the United States, China, Russia and India. It then returns to the theme of war avoidance and mutual restraint in cyberspace to see how that has played out in the policy deliberations, both national and multinational, in recent years. The paper concludes with an assessment of likely pathways, casting ahead to the 10 to 20 year time frame for international security perspectives. The paper concludes with some recommendations for policy makers to help entrench practices of mutual restraint.

Cuihong Cai

Cuihong Cai is associate professor of international relations at the Center for American Studies of Fudan University. Prior to the present job, she worked for the Foreign Affairs Office of Fudan University during 1996-2001. She received her B.S.(1993) and M.S.(1996) in biophysics, and her Ph.D (2002) in international relations from Fudan University. She also holds a B.A.(2001) in English language and literature from Shanghai International Studies University. She was a visiting scholar at the Georgia Institute of Technology in 2002, and at the University of California, Berkeley in 2007, as well as an invited fellow in the 2007 program on US National Security sponsored by the US State Department.

Cuihong Cai is the author of *Political Development in the Cyber Age* (Beijing: Current Affairs Press, 2015), *U.S. National Information Security Strategy* (Shanghai: Academia Press, 2009) and *Internet and International Politics* (Shanghai: Academia Press, 2003), as well as several dozen of articles and papers on cyber-politics, cyberspace governance, cybersecurity strategy and Sino-US relations.

Global Cybersecurity Environment: Perspectives of the US and China in Comparison

Cuihong Cai

The global cybersecurity environment can be considered as the current condition and situation related to cyberspace that affects the security, stability and development of the countries in the world. From an objective point of view, the global cybersecurity environment has many common features, such as the diversity of threats, the asymmetry of subjects, the lagging of security technologies, the absence of institutional norms, the imbalance of cyber power, the lack of collective security mechanism as well as the malfunction of the deterrence in cyberspace. These also constitute the common challenges of the global cybersecurity environment that China and the United States are facing. At the same time, the global cybersecurity environment is a subjective cognition, which has different meanings to different countries. While the United States defines global cybersecurity environment from the perspective of "threats", China tends to defines it from the perspective of "development". The threat-based approach defines it from the "others", and the development-based approach focuses more on the "self" needs, with the main purpose to enhance the development of cyberspace as well as to guarantee the domestic stability of the society. The gap of China and the United States on the global cybersecurity environment awareness leads to the difference of their cybersecurity strategy and therefore the lack of mutual trust between the two sides, which in turn becomes part of the global cybersecurity environment.

Yasuaki Hashimoto

Yasuaki Hashimoto is now Head of Government and Law Division at The National Institute for Defence Studies (NIDS) and Lecturer (International Law) at KOMAZAWA University, Japan. He also serves on the Committee on National Space Policy of Japan as ad hoc member. His educational background includes LL.B. (Kanazawa University, Japan), LL.M. (Keio University, Japan) and studies at Leiden University in the Netherlands. Professor Hashimoto's areas of expertise are international law, space law, cyber law, international law of armed conflict and international humanitarian law. He has a career spanning some 25 years and has published articles in the space law field after becoming an International Institute of Space Law (IISL) member in 1987. Particularly after joining NIDS, he is focusing mainly on the research of space law and policy from the security perspective. He also cooperates with the IISL Moot Court Competition in the Asia Pacific Region.

PRESENT SITUATION OF JAPANESE CYBER SECURITY

Yasuaki Hashimoto

The number of cyber attacks in Japan is drastically increasing. It was 3 billion in 2005, 5.7 billion in 2010, 7.8 Billion in 2012, 12.8 billion in 2013. And in 2014 the number of cyber attacks sensed in Japan jumped up to 25.6 billion, twice of the previous year 2013. And this danger is getting bigger day by day, year by year.

In fact Japan has faced some different kinds of cyber attacks. In the past, most of them were DDoS (Distributed Denial of Service) attacks to some governmental sites or commercial web sites mainly done by foreign nationalistic people. But recently more sophisticated APT (Advanced Persistent Threat) attacks are the main cyber attacks against Japan. The targets are the leading companies such as in aerospace industries, the Diet (national parliament) and Japanese diplomatic offices in abroad. Responding to such situation, Japanese government established Cyber Security Strategy in 2013. It shows that Japan has recognized the stability of cyberspace as the important national challenge. Additionally in 2014 Japanese Diet passed the Cyber Security Basic Law. Under those basic law and strategy, National center of Incident readiness and Strategy for Cybersecurity (NISC) in the Cabinet Office has played a headquarters role in the national level cyber security. This NISC, however, only monitors, analyses the cyber attacks of the government and related authorities, and coordinates the appropriate measures taken by affected organizations. The actual cyber security will be achieved by some governmental ministries and their related commercial companies groups. Japan now has this kind of multi players' cyber security structure.

Ministry of Defense also has its own Cyber Defense Unit from 2014. However, this Unit only protects the cyber networks owned and operated by Ministry of Defense(Japan Self Defense Forces) and does not cover the whole national cyber network infrastructure. It is contrastive considering the actual, real national territory is protected by Ground, Air and Maritime Self Defense Forces.

Session 2

International and Regional Responses to Cybersecurity Challenges

Tuesday, February 9, 2016

1400h - 1530h

Chairperson

Latha Reddy

Smt. Latha Reddy is the former Deputy National Security Adviser of India. She was responsible for cybersecurity and other critical internal and external security issues. She is also a Distinguished Fellow, East West Institute, New York.

She served in the Indian Foreign Service from 1975-2011. During her diplomatic career she served in Lisbon, Washington D.C., Kathmandu, Brasilia, Durban, Vienna and Bangkok. She served as Ambassador of India to Portugal (2004-2006) and to Thailand (2007-2009). She was Secretary (East) in the Ministry of External Affairs in Delhi (2010-2011) with overall charge of India's bilateral and regional relations with Asia. She was then appointed as India’s Deputy National Security Advisor in the Prime Minister's Office from 2011-2013.

Alexandra Kulikova

Alexandra Kulikova is the Global Stakeholder Engagement Manager for Eastern Europe and Central Asia at ICANN, and also acting as PIR Center Consultant (non-staff). Alexandra's research interests within the program and beyond include national and global internet governance, privacy and data protection online, state and corporate policies on ICT security, international cyber-strategies and policies.

She holds an M.Sc. degree from the London School of economics and Political Science in media and communication governance and graduate degree from Moscow State Linguistic University in theory and practice of intercultural communication and teaching foreign languages and cultures.

Working out the Rules of Global Cyberspace Governance

Alexandra Kulikova

As cyber instability increases globally, both state and non-state actors are looking for ways to elaborate ways of responsible behaviour in cyberspace, which would reduce the risk of a cyber conflict. While efforts to develop such norms and rules have been undertaken for more than a decade, various initiatives developed currently at international, regional and bilateral levels indicate stakeholders' ripe resolve to work at the prevention mechanisms in tackling cybersecurity issues. Together these efforts and initiatives form a rich ecosystem of tools and standards to ensure cyber stability serving global, regional or local goals. However, this diversity of needs, goals and agendas suggest a reconciliation as well as implementation and operability challenge.

Nandkumar Saravade

Nandkumar Saravade is the Chief Executive Officer of the Data Security Council of India (DSCI). He is a Civil-and-Environmental-Engineer-turned-IPS officer-turned-security professional. While in the IPS, he served in the state police departments of Jammu and Kashmir and West Bengal, before moving to Mumbai on deputation to the Central Bureau of Investigation in 1996.

From 2005-2008, he worked with NASSCOM (National Association of Software and Service Companies), as Director, Cyber Security and Compliance, on a three-year deputation from Public Services. In 2008, he took voluntary retirement from the Indian Police Service (IPS) and joined the private sector, leading the security and crime prevention verticals at financial institutions such as ICICI Bank and CitiBank. He was appointed as CEO of DSCI in July 2015.

International and Regional Responses to Cybersecurity Challenges

Nandkumar Saravade

Cyberspace is becoming increasingly important for nation states from policy and diplomacy perspective, given its rising strategic importance. It has emerged as fifth domain - after land, sea, air and outer space. One nation state's effort to strengthen its cyberspace capabilities evokes a response by another state. Early adopters have built up significant cyber capacity and are seemingly ahead of their counterparts. Many countries, majorly developing and underdeveloped states are in the middle of digitizing their state, economy and society. By virtue of its design, the domain in offence is dominant. Nation states and organisations are investing significant efforts and resources to safeguard their critical assets.

The cybersecurity threat landscape is changing rapidly. Dependence on cyberspace has led to the proliferation of a diverse and complex range of threats. The attacks have come of age - starting with computer registry modifying viruses to use of ransomware and complex malwares having significant kinetic impact. Technology evolution and trends such as Big data, shift to the Cloud, rising usage of Internet of Things etc. have increased overall risk exposure.

The challenges of cybersecurity are faced by one and all, and it requires concerted efforts at all layers to effectively counter the growing menace. Collaboration is required at national, regional and global level. Clearer role of established institutions, comprehensive cyber doctrines and treaties will emerge sooner rather than later, with countries signing non-aggression pacts on cyber attacks, and forging cyber-defence agreements that put cyber attacks in the same policy bucket as kinetic acts. Right from information sharing amongst trusted parties on security threats, to collaboration amongst Law Enforcement Agencies to bring cyber criminals to justice, to devising treaties and regulations for cyber domain, cyber security challenge is emerging as a big uniting factor.

Candice Tran Dai

Candice Tran Dai is Vice President and Cyberspace Program Manager at Asia Center, France. She has also been working as a consultant in international business development strategy since 2006, advising European companies regarding their market access and international development in China and Southeast Asia. Working both for the public and the private sectors, she has developed a strong expertise on ICT and Internet related issues in the Asia-Pacific region. Regarding her consulting assignments in the private sector, she has been for instance working on helping companies design and implement their digital strategies in Asian countries. In the public realm, she is focusing on issues relating to knowledge society, national ICT development strategy, as well as political and cybersecurity issues. She was besides mandated as Committee Supervisor during the 7th Asia-Middle East International session (Siamo), organized by the Institute for Higher National Defence Studies (IHEDN) in 2011 and dedicated to cyberspace strategic issues.

Economic Dimensions of National Cybersecurity Strategies in the Asia-Pacific Region

Candice Tran Dai

Many Asian governments have integrated the information and communication technologies (ICT) into their socio-economic development strategy in a way that the rapid emergence of information societies in Asia involves an increased corollary dependence upon the ICT in terms of economic prosperity. Hence, from a regional perspective, the expansion of digital economies and the development of information societies result in stronger vulnerability and greater exposure to cyber-crimes and cyber-threats, both internally and externally. The prevalence of cybercrime in the region reflects without doubt the economic vitality of the Asia-Pacific region, which has become very attractive for potential gains from cybercriminal activities. However the boundaries between what constitutes an act of crime, economic or strategic espionage are still difficult to determine. Cybersecurity has undoubtedly become a priority component in the formulation of national cyber-strategy roadmaps of Asia-Pacific countries.

At national level, Asia-Pacific countries have heterogeneous means and capabilities for prevention and fight against cyber-crimes and cyber-threats, and they have to deal with challenges of different nature with regards to cybersecurity. The result is a wide disparity in approaching the question of cybersecurity and in the formulation or reformulation of policies and / or ad hoc national strategies.

The objective of this paper is to highlight the various incentives behind the quest for indigenous cybersecurity capability and technology as a growing trend in the Asia-Pacific region, notably driven by several countries, and to show how it is intertwined with a general quest for innovation capability and a pragmatic quest for commercial objectives.

Munish Sharma

Munish Sharma is an Associate Fellow with the Cybersecurity Project at IDSA. He is an engineering graduate and holds a masters in Geopolitics and International Relations. Prior to masters he worked as software engineer for four years with Accenture Services. His research areas are Cybersecurity, Critical Information Infrastructure Protection, Space Security, and Defence Technologies.

Cherian Samuel

Cherian Samuel is Associate Fellow in the Strategic Technologies Centre at the Institute for Defence Studies and Analyses. His recent publications include *India's International Cybersecurity Strategy in Cybersecurity: Some Critical Insights and Perspectives*, Damien D. Cheong ed, S. Rajaratnam School of International Studies, Singapore (January 2015), *Net-Centric Defence Forces : A Macro View* in DSA Magazine, July 2014 issue, *Cyber security and National Development* CASS Journal, Vol. 1, No. 3, July–September 2014 ((Pune), *Cybersecurity and Cyberwar*, (October 2013 issue of Seminar magazine), and *Prospects for India-US Cyber Security Cooperation*, (Volume 31, Issue 2, Strategic Analysis September 2011). His monograph *Global, Regional and Domestic Dynamics of Cybersecurity* was published in December 2014. He was co-ordinator of the IDSA Task Force on Cyber Security which published a report on *India's Cyber Security Challenges* in March 2012.

A South Asian Regional Cybersecurity Cooperation (SARCC) Forum: Prospects and Challenges

Munish Sharma and Cherian Samuel

South Asia has experienced a long haul of robust economic growth, and World Bank statistics conclude that it has been among the fastest-growing regions in the world. Much of this economic development has been facilitated through the advances in information technology with the digitization of public services and opportunities for business development in Information and Communication Technology. However, countries in the region are yet to internalize cyber security as essential to their economic, political and national well being. Lack of capabilities and capacities to understand and remediate threats make not just individual countries, but the entire region vulnerable to threats from state and non-state actors.

As an economic and geopolitical organisation of eight countries, South Asian Association for Regional Cooperation (SAARC) can play a pivotal role in capacity building as well coordinating cyber security efforts of all the members facing non-traditional security threats from non-state actors to both their populace and businesses, in form of terrorism, cyber crime etc. The paper examines the feasibility of SAARC putting across Cyber security as a key agenda item for cooperation, given the divergences among members over traditional security threats. It makes an attempt to draw learning lessons from the ASEAN Regional Forum (ARF) to address Cyber issues as key security matter to ensure a safe and secure Cyberspace across South Asia.

Session 3

Non-State Actors and Cyberspace

Tuesday, February 9, 2016

1600h - 1730h

Chairperson

Ravi Kant

Shri Ravi Kant is the Additional Secretary in the Ministry of Defence. He is a 1984 batch IAS officer from the Bihar cadre. Before taking charge as Additional Secretary, he served as Joint Secretary with Department of Defence Production in the Ministry of Defence.

Alok Vijayant

Alok Vijayant is Director-Information Dominance Group and Tech Financial Intelligence Unit of the National Technical Research Organisation (NTRO).

Asymmetrism in Cyberspace: State vs. Non-state Actors

Alok Vijayant

The asymmetries in the fifth domain of cyber lend itself exploitable by all and sundry. The distinction between the state and the non-state actors have got marginalised in the current decade and is the non-state actors that call the shots and the state actors only try to legislate the domain and create controls to have stakes in this domain.

What remains to be seen is whether coercive and deterrence techniques would be the parameters to reckon with or there are other methods of controls. Primarily non-state actors target systems and entities that could bring benefits to them. Most of the time their target focuses on money, prestige, glorifications and alike rather than focussing on CII and other critical systems. Such systems would only be targeted in case of a personal revenge that they might have on their folds due to small amount of bills or any mundane issue, or in the event someone is willing to sponsor the act, be it the state or corporate. However, state agencies would dwell into investments in offensive technology for various acts of espionage, foreknowledge, diplomacy and warfare.

Sanjeev Relia

Sanjeev Relia was commissioned into the Corps of Signals in 1986, he holds a B.Tech in Electronics and Telecommunications. He attended the Defence Services Staff College Course in Wellington. Col. Relia has been associated with modernization of IT and communication infrastructure in the Indian Army and issues related to Cyber Security. Besides research work, he is also pursuing Ph.D on *India's Cyber Security Challenges*. He was associated with research project at The United Services Institution of India, and authored the book *Cyber Warfare: It's Implications on National Security*, published in November 2015. He is a certified Ethical Hacker and holds a Post Graduate Diploma in Cyber Laws.

Non-State Actors and Cyberspace: An Overview

Sanjeev Relia

Millions of dollars are lost because of cybercrime every year. That is perhaps the reason that cybercrime is the most reported and discussed facet of cyberspace. Yet cyber-criminals are not the ones who pose the gravest of threats. It is the threat of presence of non-state actors in cyber domain that is worrying nations today. The very nature of cyberspace makes them a potent force that will play a pivotal role in any future cyber war.

The paper focuses on defining who the Non State actors in the cyberspace are and how non state actors operating in the virtual world (cyberspace) are different from the non state actors operating in the real world. It is also discussed in detail the modus operandi of Cyber militia and Cyber-terrorists and the threats that a country like India faces from non state actors operating in the cyberspace.

Arun Mohan Sukumar

Arun Mohan Sukumar heads the Observer Research Foundation's Cyber Security and Internet Governance Initiative, coordinating research projects on internet governance, data protection, and international norms. He is the elected vice-chair of the Asia-Pacific Internet Governance Forum. Arun is a lawyer by training, educated at NALSAR University of Law, Hyderabad. He holds a Master's degree from the Fletcher School of Law and Diplomacy, Tufts University, where he was the Douglas Dillon Fellow, and the recipient of the Leo Gross Prize for Outstanding Student of International Law. Arun was previously Senior Fellow at the Centre for Communication Governance, National Law University Delhi, working on global internet governance. He has served on the editorial board of The Hindu, and continues to write for the daily on foreign affairs.

State and Non-State: Residual Actors in Cyberspace

Arun Mohan Sukumar

The non-state actor shares an adversarial relationship with existing international regimes on cybersecurity and cyber warfare. This is true of many international regimes today, whether they relate to non-proliferation or maritime piracy. Multilateral instruments and organisations founded in the aftermath of the Second World War have tried "manage" non-state actors, often treating their actions through the prism of the state. The etymology of the phrase itself is revealing: "non-state" refers to all actors excluding the nation-state, which remains the primary agent in international relations. This trend is visible even in conversations around cyber security regimes, notably in the effort to create norms around "attribution" of non-state actions. Cyber security regimes, however, cannot afford to treat non-state actors residually.

Individuals in cyberspace possess hard and soft capabilities that go well beyond any other common space regulated by international law. The problem of absorbing non-state actors into international regimes is complicated by the fact that cyberspace is not a "commons" in the true sense of the world. Unlike the high seas, the ozone layer or outer space, the internet is heavily regulated by national, regional and local laws that confer rights and responsibilities on the individual. So while the state retains agency over many actions of a non-state actor in cyberspace, international regimes have to be sensitive to the different legal and technical standards that limit universal treatment. This paper explores if existing cyber norms have been able to adjust to these differing standards, using the example of the Tallinn Manual and the 2015 report of the UN Group of Governmental Experts. Both instruments are non-binding, but constitute definitive attempts to codify norms on state and non-state conduct in cyberspace.

Gillane Allam

Gillane Allam is a career diplomat of the Ministry of Foreign Affairs of Egypt. She is a graduate of the School of Economic and Political Sciences of Cairo University. She later pursued her graduate Studies at the Woodrow Wilson School for International & Public Affairs of Princeton University, USA as a Parvin Fellow through a Fulbright Fellowship.

During her service abroad , Allam served as a diplomat in the Permanent Missions of Egypt to the UN in New york & Specialized Agencies in Vienna. She held the posts of Ambassador consecutively to India, Australia, New Zealand & countries of the Pacific. She was awarded the Order of The Republic of Egypt for Professional Distinction.

Post retirement, she taught at the Graduate School of The Arab Academy in Cairo. She also joined the Egyptian Council for Foreign Affairs (ECFA). She represented ECFA, participated & contributed to a multitude of conferences, seminars, workshops on regional & international issues related to terrorism, non proliferation & regional security.

NON-STATE ACTORS & CYBERSPACE- A NORTH AFRICAN PERSPECTIVE

Gillane Allam

In the geopolitical and geostrategic realm, Non State Actors (NSAs) are not a novel phenomenon in Asia. Mainly since the early 1980s, from countries of West Asia or what is called the larger Middle East, news of operations of Hezbollah, Hamas, Taliban, Al Qua'ida swamped all international media domains.

The more recent events since 2010 of the so called Arab Spring in countries of West Asia and North Africa gave upstage appearance for an additional variation of armed NSAs (ANSAs) notably DA'ESH (otherwise called ISIL/ ISIS/ IS).

The question arises if DA'ESH with its modus operandi inclusive of Cyberspace is a threat to Asia's ambitious economic progress. The reply is in the affirmative. DA'ESH names itself the CYBER CALIPHATE.Political stability and sustainability of flow of energy is primordial to economic growth. UNSCR 2253(2015), as an attempt at suppressing and drying off financial resources available to DA'ESH, will be a long term efficient way of breaking its might. Fighting it in Cyberspace might be another more lethal approach. Egypt as a non-permanent member of UNSC for the years 2016-2017, while undertaking its responsibilities as Chairman of UNSC Counter Terrorism Committee for that period, will seek international support in that mission. Furthermore, the Fatwa Authority of Egypt has established a strong multilingual Internet Blog with a view to modernize the Islamic approach and address to society as well as dispute and disqualify calls for radicalization. Asia's booming economies and its Cyberspace knowledge and industry should be at task in these endeavours.

Keynote Address

Wednesday, February 10, 2016

1000h - 1100h

Keynote Address

Arvind Gupta

Dr. Arvind Gupta is the deputy National Security Adviser of India. He is also the Secretary in the National Security Council Secretariat (NSCS), an apex advisory body tasked with suggesting to the government on political, economic and strategic security concerns. Previously, Dr.Gupta was the Director General of Institute for Defence Studies and Analyses (IDSA) from 5th January, 2012 to 7th August 2014.

He holds a Ph.D in International Relations from Jawaharlal Nehru University, New Delhi; M.Sc. in Physics from Delhi University. He was Visiting Member at the Tata Institute for Fundamental Research (1974-76) and served at the Oil & Natural Gas Commission (1976) and at the State Bank of India (1976-79) before joining the Indian Foreign Service in 1979.

Arvind Gupta retired from the Indian Foreign Service in 2013. Dr. Gupta has worked in the Ministry of External Affairs in different capacities and served in diplomatic missions in Moscow, London and Ankara. He held the Lal Bahadur Shastri Chair on National Security at the IDSA from 2008 to 2011.

Prior to joining the IDSA, he was Joint Secretary at the Indian National Security Council Secretariat from 1999 to 2007. During his tenure at the NSCS, he dealt with a wide range of international and national security issues and participated in the various working groups and task forces set up by the National Security Council. He has also worked with the Kargil Review Committee.

Session 4

Securing Strategic Critical Infrastructure

Wednesday, February 10, 2016

1130h - 1300h

Chairperson

ALHAD APTE

Shri Alhad Apte was the Chairman of National Technical Research Organisation (NTRO). He joined NTRO in the month of April 2012 as Senior Advisor, the Second in Command of the Organisation. He took over as Chairman, NTRO on July 01, 2013. Shri Apte is recipient of Special Contribution Award of Department of Atomic Energy (DAE) in 2007.

He joined Bhabha Atomic Research Centre (BARC) as Scientific Officer in the year 1972. During his tenure at BARC, he held important portfolios and served for 40 years. He retired on attaining the age of superannuation on 30th April, 2012 as an Outstanding Scientist and Head of Computer Division of the BARC. He also chaired Computer and Information Security Advisory Group of DAE. He undertook and completed several DAE level projects, including classified projects. He has worked on Cyber Security Related Consultative Committee of the International Atomic Energy Agency. He was closely involved with CERN, Geneva and European Commission projects in Grid Computing.

TED LEWIS

Ted Lewis is a computer scientist and author of the book *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*. His unique scientific approach to the field of critical infrastructure protection uses network theory, optimization theory, and simulation software to analyze and understand how infrastructure sectors evolve, where they are vulnerable, and how they can best be protected.

Ted Lewis was Professor of Computer Science and Executive Director of the Center for Homeland Defense and Security at the Naval Postgraduate School in Monterey, California. He has advised the governments of Taiwan, Egypt, Mexico, and Italy in the areas of economic development and technology development parks. He has previously held a variety of positions within IEEE Computer Science (EIC of IEEE software, EIC of IEEE COMPUTER), industry (CEO Daimler Chrysler Research and Technology NA, Senior Vice President of Eastman Kodak) and academia (University of Louisiana, Oregon State University, Naval Postgraduate School). Lewis is the author of over 30 books and 100 papers on computing, critical infrastructure and complexity.

Challenges of Cybersecurity: Malware and AS-level Structure

Ted Lewis

There are many policy and technical challenges facing the security of cyberspace. This paper proposes a technical solution to only two challenges having to do with the spread of malware, a process that is similar to the spread of a contagion within a human or animal population. The monoculture design and scale-free structure challenges posed by the AS-level Internet promotes widespread contamination even under very small probability or vulnerability to an exploit. On the other hand, the scale-free structure of the AS-level Internet can be turned to a defender's advantage by relating resilience to vulnerability and self-organization as measured by spectral radius. The author shows that resilience increases with decreases in vulnerability, spectral radius, or both. Furthermore, an analysis of the AS13579 Internet identifies 944 (7%) of the AS-level nodes as blocking nodes. By protecting these blocking nodes, spectral radius is dramatically diminished, with corresponding increase in resilience. A second application of blocking node analysis shows that protecting 13.5% of the global Internet's AS-level nodes can eliminate nearly all malware.

Kah-Kin Ho

Kah-Kin Ho has been with Cisco for more than 18 years and in his current role as the Head of Strategic Security, a position he has held since January 2014, he plays a key role in developing and shaping Cisco's strategic positioning in security that aligns with customer requirements. He also serves in the Advisory group of EUROPOL European Cyber Crime Center (EC3) and teaches Cyber Security Strategy and Policy at Eidgenössische Technische Hochschule (ETH), Zürich.

EVOLVING ROLE OF GOVERNMENT IN CRITICAL INFRASTRUCTURE PROTECTION

Kah-Kin Ho

The 21st century has so far signaled an era of wide-scale deregulation and privatization, with much of the nation's critical infrastructures (energy, transport, finance, medicine) now in the hands of the private sector. These critical infrastructures are constantly targeted by adversaries ranging from non-state actors such as terrorist groups, hacktivist groups, organized criminals, etc. to state actors, and due to our high degree of interconnectedness across the globe. Part of the reason why it can be difficult to secure critical infrastructures is due to the divergence of interests between the private and public sectors. The private sector's primary focus is corporate efficiency: in terms of security, implementing the bare minimum level of security, since its main goal is profit-making. The government, in contrast, is principally concerned with achieving social order, national security and economic prosperity for its population. Yet governments today do not provide close supervision of, or operational control over, these critical infrastructures that now fall within the realm of the private sector. As a result, it has been argued that the role of government as the legitimate provider of security has diminished, and that it will continue to weaken moving forward. This paper provides the argument that the role of government in helping to secure critical infrastructure is ever more critical but their remit must transcend what their historical regulatory role has typically entailed. To formulate a viable approach going forward, a new framework will be proposed through which governments must strategize, and they must be ready to draw upon analogous lessons learned from past preparedness efforts geared towards other areas of threat, such as pandemic and terrorism.

Jana Robinson

Jana Robinson is currently Space Security Program Director at the Prague Security Studies Institute (PSSI). She previously served as Space Policy Officer at the European External Action Service (EEAS) in Brussels. She was also a Space Security Advisor to the Czech Foreign Ministry, seconded to the EEAS. From 2009 to 2013, Ms. Robinson worked as Resident Fellow at the European Space Policy Institute (ESPI), seconded from the European Space Agency (ESA), leading the Institute's Space Security Research Programme. Prior to joining ESPI, she served as Development Director at PSSI from 2005 to 2009, and administered its affiliate organization in Washington DC, PSSI Washington. She holds an MA in Asian Studies from George Washington University's Elliott School of International Affairs, and an MA in Chinese Studies from Palacky University. She received scholarships to attend the International Space University's (ISU) 2009 Space Studies Program (SSP09), the 2008 Summer Training Course at the National Taiwan Normal University in Taipei, and a one-year course of study at Shanghai University 1999-2000.

Governance Challenges at the Intersection of Space and Cybersecurity

Jana Robinson

Despite the critical role of the cyber and space domains for national security and war-fighting, decision-makers still struggle to configure proper crisis management mechanisms, including the rapid crafting of proportionate responses to any hostile or disruptive actions by certain space-faring or other nations. Understanding the cross-domain parallels as well as differences is essential to the successful safeguarding of both of these domains. Accordingly, this paper will examine how the cyber and space domains interact (e.g. the transmission of cyber signals by satellite communications systems), the vulnerabilities associated with how they connect (e.g. cyber attacks on space systems), and possible risk-mitigation strategies. It will focus on common features, as well as distinct characteristics, of these domains, and how they impact on political / military decision-making.

Understanding the different physical and technical properties of the two domains is also the key when seeking to arrive at appropriate policy prescriptions.

Active involvement of both government and private sector actors is required to address common threats and to formulate realistic norms and guidelines for responsible behaviour in these two domains. Such norms, as well as transparency and confidence-building measures (TCBMs), are of critical importance for arenas where traditional arms control methods cannot be easily employed. As in other fields, the establishment of strong communication links between relevant authorities, including hotlines, exchanges of information concerning policies and doctrines and regular dialogues among decision-makers are all foundational TCBMs that enhance security. The intersections of cyber and space remain on the rise and require urgent attention and contingency planning and preparation if the essential services offered by both domains are to be protected and preserved.

Caroline Baylon

Caroline Baylon is a researcher on cybersecurity. She is currently carrying out two research projects, one on curbing the proliferation of cyber weapons and another on cyber proxy armies, funded by the UK government. She serves as the director of the cybersecurity research program at the Center for Strategic Decision Research in Paris, France and was previously the lead researcher on cyber security at Chatham House (The Royal Institute of International Affairs) in London, United Kingdom. While there, Caroline's research focused on critical infrastructure protection, notably on cyber security challenges for nuclear facilities and on cyber security threats to satellites. She was also the editor of the Journal of Cyber Policy, a peer reviewed academic journal published by Routledge, Taylor & Francis and served on the secretariat of the Global Commission on Internet Governance. She speaks regularly at international conferences and is a frequent media commentator and contributor. Caroline will be joining AXA, which is establishing a think tank on cyber security within the organization, in April. Caroline holds a Master of Science in Social Science of the Internet from Balliol College, University of Oxford and a Bachelor of Arts in Economics from Stanford University.

Cyber Security Threats to Critical Infrastructure: A Case Study of Nuclear Facilities

Caroline Baylon

Perhaps the greatest cyber security issue facing the nuclear industry is that many in the sector do not fully understand the risk, and therefore a key first step is to develop guidelines to assess and measure this risk as accurately as possible. This will help CEOs and company boards to understand what is at stake, and also provide them with a clear economic rationale to invest in cyber security. The development of cyber insurance, with its strong reliance on risk metrics, may be an important tool for promoting the development of cyber risk guidelines. In tackling the challenges related to the "human factor", it will also be important to raise awareness among both engineers and contractors of the risks involved in setting up unauthorized connections or plugging in personal USBs at nuclear facilities. Measures that promote disclosure and information-sharing can also play an important role in enhancing cyber security, as can regulatory standards and other policy measures, improved communication to bridge cultural divides and the implementation of technical solutions.

A. Vinod Kumar

A. Vinod Kumar is an Associate Fellow at the Institute for Defence Studies and Analyses (IDSA), New Delhi and a visiting faculty at the Institute of Foreign Policy Studies (IFPS), University of Calcutta, Kolkata. His areas of expertise include nuclear policy issues, missile defence, foreign policy and strategy. Kumar's first book titled India and the Nuclear Non-Proliferation Regime - The Perennial Outlier was published by the Cambridge University Press in April 2014. He has written extensively in acclaimed publications like Bulletin of the Atomic Scientists, The National Interest, Strategic Analysis, Asia Times and Vayu Aerospace Review, among others. Prior to joining IDSA, Kumar was a journalist with some leading Indian media houses, including as Executive Editor of South Asia Monitor - a media diplomacy platform. He was also a Fellow at the Indian Pugwash Society. His ongoing study is on the implications of missile defence for nuclear deterrence. Concurrently, he is also spearheading an archival mining and documentation effort to trace the history of India's nuclear programme as part of the Indian Nuclear History Project at IDSA. Kumar is recipient of the Ministry of Defence Madras Medal.

Securing Critical Infrastructure from Cyber Threats: Developing Defence, Deterrence and Norms

A. Vinod Kumar

How should a cyber attack on a nation's critical infrastructure be described - as a subversive action or an act of war, or rather a proxy war. Cyber-attacks, on individuals as well as public utilities, have been integral to the spectacular growth of cyber platforms and dependence on digital technologies in the recent past. While intrusion and disruption has hitherto been the hallmark of such attacks, numerous calibrated attacks in recent years on critical infrastructure (including strategic assets) of various countries underline the new dimensions and frontiers of warfare, involving "adversarial forces" that blur conventional combatant identities. While the deployment of non-state actors for transnational cyber attacks highlight the element of proxy conflicts in this spectrum, that states are forming techno-military groups (cyber commands) reveals the truism of cyberspace evolving into the new battleground. This paper is an attempt to conceptualize this battlefield and the threat environment, while pointing to its numerous complexities: (a) objectives of the attack, rather than the type of actors, define the nature of this neo-warfare; (b) episodes like Stuxnet, involving attacks on nuclear infrastructure, points to outcomes evolving towards mass subversion, destruction and instability of states; (c) that conventional deterrence doctrines may not suffice as cyber-attacks run short of triggering a full-fledged war nor revealing belligerence; (d) norms are non-existent, or instead might buttress subversion, as state actors use plausible deniability and virtual camouflage in a porous domain to endow cyber warfare with the same attributes or flexibility of terrorism.

Session 5

Cybersecurity and the Digital Economy

Wednesday, February 10, 2016

1400h - 1530h

Chairperson

V.K. Saraswat

Dr. V.K. Saraswat is one of the full-time members of NITI Aayog. He was a Former Secretary of Defence (Research & Development). He also served as a Director General of Defence Research and Development Organisation (DRDO) and as Scientific Advisor to Defence Minister. He was conferred the Padma Shri in 1998. He was also conferred the Padma Bhusan by the Government of India in 2013. Dr. Saraswat has been credited with development of Liquid Propulsion Rocket Engines and missiles namely PRITHVI, DHANUSH, PRAHAAR indigenously. He is also the principal architect of the Ballistic Missile Defence programme which included major technology breakthroughs.

Dr. Saraswat's efforts have led to establishment of Research & Innovation Centre at IIT Madras; MILIT- Centre for Training needs of armed forces on S&T; CERT for reporting, auditing and handling emergency response of Information Security Incidents; CHESS - futuristic technology Centre for High Energy Laser and Microwave devices; Kyrgyz-Indian Mountain Bio-Medical Research Centre at Kyrgyzstan.

Dr. Saraswat has a Masters in Engineering from IISc Bangalore and a Ph.D from Osmania University.

Liam Nevill

Liam Nevill is currently working in the Australian Strategic Policy Institute's International Cyber Policy Centre, researching and writing on international and domestic cyber policy issues. Prior to joining ASPI Liam worked at the Australian Department of Defence on strategic and international defence policy issues. He has previously worked in policy roles in the Department of Health and Ageing, and the Northern Territory Treasury. Liam holds a Master of Arts in Strategy and Security, and a Bachelor of Arts in History, Politics and International Relations, from the University of New South Wales.

Challenging Opportunities for Asia-Pacific's Digital Economy

Liam Nevill

The Asia-Pacific region offers a diverse set of opportunities for the continued growth of the digital economy. The region is home to some of the largest and most advanced economies, and some the least connected and least developed. The size, population, demography and economy of the region provides significant opportunity to harness the connectivity that cyberspace enables to enhance productivity and diversify practices and markets. The digital economy consistently grows as a percentage of region's GDP every year, and the adoption of innovative and disruptive business models that take advantage of technologies including big data analytics and mobile devices will likely see this continue. However challenges remain to greater growth, specifically cybercrime and legal and regulatory practices that have failed to keep up with new business models. Addressing these will enable greater growth, and assist in the development of the region's least developed countries.

Madan M. Oberoi

Madan M. Oberoi is an Indian Police Service (IPS) officer of 1992 batch. He is presently deployed as Director of Cyber Innovation and Outreach Directorate in the INTERPOL Global complex for innovation (IGCI), Singapore. He supervises two sub-directorates including 'Strategy and Outreach' and 'Research & Innovation'.

New Technologies and New forms of Crime Need to Recalibrate Law Enforcement Strategy / Procedures / Law

Madan M. Oberoi

Although predicting the future can be uncertain, it is important to understand the new technology trends. From a law enforcement perspective it is equally, if not more, important to understand the way technology is going to impact Criminal Justice System and its stakeholders namely law enforcement agencies, prosecutors and judiciary and also the world within which Criminal Justice System operates. We need to understand technology's potential use by police as well as it's exploitation by criminals and terrorists.

This paper attempts to understand some of the current technological trends like Data Tsunami, Smart Everything, Digital Disruption and Cyber Insecurity. In light of these shifts, the paper looks at their impact on Intelligence gathering, Investigation, Police Information Management, Training for Policing and Third-Party Policing.

The paper looks at criminals' exploitation of technology by using it for secure and anonymous communication, leveraging technology for a wider reach, for laundering proceeds of crime, for hiding their footsteps by using anti-forensics, crowdfunding their illegal activities, accessing new markets for illegal products, motivation and recruitment of new criminals / terrorists, and new business model of crime-as-a-service.

Finally the paper attempts to suggest recalibration of existing policing strategies and procedures in light of availability of expertise, information and resources as well as in light of growing multi-jurisdictional nature of new crimes.

IL Seok OH

IL Seok, OH is Senior Researcher at Institute of Legal Studies, Korea University Law School, an expert in Contract, Tort, Oil and Gas Law, and Information Security Law. He has a Ph.D from Korea University and an LLM from the Northwestern University School of Law, Chicago. Among his published works are Recommendations on Reforming Critical Information Infrastructure Protection Act of Korea with a View from Risk Allocation, Designing Effective Responding Legal and Political Measures against North Korea's Cyber Attacks, and Establishment of Efficient Countermeasures against Cyber Attacks without Applying 'Law of War'.

KOREAN LEGAL INITIATIVES TO COMBAT CYBERCRIME AND ENHANCE DIGITAL ECONOMY

IL Seok OH

Computer networks and information systems have governed daily human lives in this early 21st century and provided so many advantages. However lots of cyber attacks and cyber crimes have made damages against critical computer systems and disturbed their functions. It is very difficult to find out the causes and results of the cyber crimes and to respond against the risk properly. Therefore a state shall design appropriate legislations and national plans to respond against cyber crimes and enhance digital economy.

In Korea, to protect critical information infrastructures from cybercrimes, "Critical Information Infrastructure Protection Act" has been enacted since 2001. An act on "Promotion of Information and Communications Network Utilization and Information Protection" has been enacted to contribute to the improvement of citizens'lives and the enhancement of public welfare by facilitating utilization of information and communications networks, protecting personal information of people using information and communications services, and developing an environment in which people can utilize information and communications networks in a sounder and safer way.

"Electronic Financial Transactions Act" has been enacted to contribute to ensuring the security and reliability of electronic financial transactions by clarifying their legal relations and to promoting financial conveniences for people and developing the national economy by creating a foundation for the sound development of electronic financial industry.)

The paper will introduce major cyber attacks and cybercrimes happened in Korea and Korean government's policies and activities to combat cybercrimes. The detailed provisions of the above Acts are explained and recommendations are proposed to amend the Acts to make it more efficient measures to combat cybercrime in Korea.

Uchenna Jerome Orji

Uchenna Jerome Orji is an Attorney admitted to the Nigerian Bar as a Barrister and Solicitor of the Supreme Court of Nigeria. He holds an LL.B Honours Degree from the University of Nigeria and, an LL.M Degree from the University of Ibadan, Nigeria, where a major part his research focused on Cybersecurity governance. He is currently completing a PhD in law at the Nnamdi Azikiwe University in Nigeria, with a specialization in telecommunications regulation. Uchenna is also a Research Associate at the African Center for Cyber Law and Cybercrime Prevention (ACCP) located within the United Nations, African Institute for the Prevention of Crime and the Treatment of Offenders in Kampala, Uganda. He is the author of *Cybersecurity Law and Regulation* (Wolf Legal Publishers: The Netherlands, 2012), in addition to several journal publications on cybersecurity law and also works as a consultant for a number of local and international organizations.

Regionalising Cybersecurity Governance in Africa: An Assessment of Responses

Uchenna Jerome Orji

Since the beginning of the Millennium, Africa has continued to witness a phenomenal growth in Internet penetration and the use of Information Communications Technologies (ICTs). However, while the spread of ICTs and Internet penetration has been enhancing development in Africa, there have also been concerns about cybersecurity. To address these concerns, several African intergovernmental organizations have developed legal frameworks to promote cybersecurity. At the sub-regional level, the Economic Community of West African States (ECOWAS) adopted a Directive on Fighting Cybercrime in August 2011, while the Common Market for Eastern and Southern Africa (COMESA) adopted a Model Cybercrime Law in October 2011. In March 2012, the Southern African Development Community (SADC) also adopted a Model Law on Computer Crime and Cybercrime. At the regional level, the African Union (AU) adopted the AU Convention on Cyber Security and Personal Data Protection in June 2014.

This paper seeks to discuss these regional legal instruments with a view to determine their impact on the development of national cybersecurity laws within the African region. In particular, the paper will examine whether these instruments have provided an effective basis for legal harmonization and international cooperation while also considering the challenges to the regionalization of cybersecurity measures. The paper will also propose measures to enhance the effectiveness of regional cybersecurity instruments including the development of follow-up mechanisms, mutual legal assistance mechanisms and incident response mechanisms to enhance regional cooperation in the coordination of responses to cybersecurity incidents.

Session 6

Role of Military in Cybersecurity

Wednesday, February 10, 2016

1600h - 1730h

Chairperson

PRAKASH MENON

Lieutanant General Prakash Menon was a military adviser to the National Security Advisor. He has also been a commandant of the prestigious National Defence College, New Delhi. During his service, the general has earned the reputation of a “Soldier Scholar”. He has been an outstanding Commander in the field. His command at the Battalion, Brigade and Divisional levels in counter insurgency environment of Jammu and Kashmir has been commendable; earning him two military awards for distinguished service. As a company commander in 1989, he was awarded for his performance during active operations on the Siachen Glacier. He has been awarded a Ph.D for his thesis on *Nuclear Deterrence and Limited War in the Indo Pak context* by the Madras University. He was nominated by the then Cabinet as a member of the expert group for establishment of the Indian National Defence University (INDU).

Liina Areng

Liina Areng assumed the duties of Head of International Relations at Estonian Information System Authority in March 2014. Prior to her current position, she coordinated NATO Cooperative Cyber Defence Centre of Excellence's (NATO CCD COE) international affairs. She holds an honorary title of NATO CCD COE Ambassador.

Between 1999 and 2012, she held different positions in Estonian Ministry of Defence. Her last appointment in the Ministry was Senior Cyber Security Adviser. During 2007-2010, Liina Areng worked as Assistant Defence Counsellor at the Permanent Representation of Estonia to NATO. Her previous positions include being Arms Control Adviser (2005-2007) and Chief Expert on Russia and the Commonwealth of Independent States in Defence Policy and Planning Department (2000-2005).

ROLE OF MILITARY IN CYBERSECURITY

Liina Areng

The military dominance of traditional great powers has caused adversaries and competitors to adapt in a variety of ways to confront this strategic advantage. Cyber capabilities are most notably used as a tool to gain leverage in international security, challenging the traditional military capabilities and doctrine. To immobilize a nation, to render it incapable of defending itself, attackers no longer need kinetic weapons. A cyber attack against national critical infrastructure could have a cascading effect to economy, society and government in ways difficult to understand, model or predict. The failures in ICT can have serious national security implications, yet the response to cyber threats cannot be conceived purely in terms of classical warfare.

The analysis will discuss the need to defend the society as an “ecosystem” by orchestrating military planning and preparation for civil emergencies. While nations are developing their arsenals of defensive and offensive cyber weapons, most cyber problems remain in the "gray area" beneath clear military action, response to which needs proper preparedness and resilience, but also adequate international containment and de-escalation mechanisms.

Amit Sharma

Amit Sharma is currently serving as Additional Director in the Office of the Scientific Advisor of Defence Minister, Defence Research and Development Organization (DRDO), Ministry of Defence, Government of India. He has worked in the field of Information Security, Information warfare, Strategic Information Dissemination Systems, Net Centric Warfare, C4I2SR systems and Secure and survivable networks. He is a Chevening Scholar and gained his Masters in 'Global Security' from Defence College of Management and Technology, UK Defence Academy, United Kingdom. He did his B Tech (honors) in Computer Science and Technology from National Institute of Technology, Hamirpur, India.

His most recent publications includes, *Cyber Wars: A paradigm shift from means to ends; Asimit - A virtual architecture for wide area file system; BBN approach for vulnerability assessment of strategic information dissemination systems*; *Xcalibur- A dynamic protocol for authentication and secure communication based on dynamic key construction and cryptographic algorithm selection*; etc.

THE TRIAD THEORY OF CYBER WARFARE: A FRAMEWORK FOR STRATEGIC CYBER WARFARE

Amit Sharma

Information assets is a strategic enabler or force-multiplier that has revolutionized the contemporary age to an extent that this age is often termed as an Information age, nevertheless it has also induced a strategic vulnerability in our critical assets which in current scenarios is exploited by a new form of warfare called the strategic cyber warfare.

This strategic vulnerability to cyber warfare is based on inducing strategic paralytic effect upon the victim nation by performing rapid decisive operations to gain rapid domination in cyberspace. The author believes that such a strategic paralytic effect can be induced onto the victim nation if the Clausewitz's Trinitarian warfare is performed in cyberspace. This paper tries to define a strategy, The Triad Theory of Cyber Warfare, which aims at destroying the elusive Clausewitzian trinity in cyberspace by performing parallel warfare in cyberspace, so as to gain rapid dominance and strategic freedom of operation, consequently resulting in the destruction of the victim nation as a system of systems.

The paper also analyses the critical components to be targeted in waging strategic cyber warfare and provides satisfactory reasons for failure of contemporary cyber attacks to generate a strategic effect. The analysis is concluded with the presentation of a framework of strategic cyber warfare involving The Triad Theory of Cyber warfare; its operational cyber campaign plan and formation of a 'Known' and 'Credible' Cyber deterrence to generate a scenario of Mutually Assured Destruction in cyberspace thus guaranteeing a strategic status quo, as the primary means of achieving grand strategic objectives in the contemporary world order. Once the strategic aspect of the cyber warfare is established, the author will conclude by providing various recommendations for creation of cyber deterrence capabilities especially involving the notion of Prepare, Pursue, Protect and Prevent in cyberspace to capitalize the strategic opportunities provided by this framework of strategic cyber warfare.

Caitriona Heinl

Caitriona Heinl joined the Centre of Excellence for National Security (CENS) at S. Rajaratnam School of International Studies (RSIS) as a Research Fellow for cybersecurity issues in October 2012. She has published articles in peer-reviewed journals and policy advisory reports on topics that include international and regional cooperation, country case studies, national security implications of emerging technologies such as cyber capabilities and increasingly autonomous technologies, public-private partnerships, and cyber defence.

International Military Cyber Cooperation in Asia

Caitriona Heinl

The paper focuses on the following aspects relating to International Military Cyber Cooperation in Asia.

i) Particular issues that face militaries in Asia in terms of cyber; including the relevance of international civil-military and law enforcement cooperation;

ii) Status of cyber policy within the regional military institutional structures, with specific focus on the ADMM / ADMM Plus and other regional networks;

iii) Recommendations on where there is space to move forward to increase cooperation;

iv) Good practices in other regions that may be adapted to suit the region;

v) Where India fits in this dialogue.

Li-Chung Yuan

Li-Chung Yuan is currently teaching at the Graduate Institute of Strategic Studies in the Republic of China (ROC) National Defense University (NDU) as an Assistant Professor with the rank of Colonel. He received his MS from Iowa State University with major in Transportation, and MA in the International Master Program in Taiwan Studies from National Chengchi University in Taiwan. He acquired his PhD from Department of War Studies at King's College, London. As for military educational background, he graduated from ROC Air Force Academy and attended the Electronic Warfare Advanced Course in Taiwan's military. With 22 years of military service, he served as teaching assistant and squadron commander in the Air Force Academy, translation officer at the Institute of National Strategic Studies (a defense think tank), staff officer at the Intelligence Division (J-2) of the Ministry of National Defense, Air Combat Command, and the Combined Logistics Command. He is serving in the editorial board of the journal Strategic Vision (in English) and National Defense Magazine (in Chinese).

ROLE OF MILITARY IN CYBERSPACE: CASE OF REPUBLIC OF CHINA (TAIWAN)

Li-Chung Yuan

Cyberspace has been utilized in various fields of national development as a whole information infrastructure, including the military. There is no exception for both China and the Republic of China (Taiwan), in that military confrontation between two sides still exists and cyberspace is an essential part of the confrontation. Tension in the Taiwan Strait has apparently given way to a potential conflict in the cyber-domains; thus, Taiwan government has been the crucial target of cyber espionage and attacks suspiciously sponsored by China. This means that cyber threats below the level of "war" should be dealt with in serious manner.

Nevertheless, issues have been addressed with regard to the appropriateness of using the armed forces to tackle threats of, inter alia, sabotage, subversion, and especially espionage in cyberspace. There are advantages of using the military to play such role. Most militaries in advanced nations possess certain level of cyber capability to either support the fighting in the battlefield or defend their own systems during peacetime. Using Taiwan's armed forces as the case, this paper will explore the roles played by military in various fields of cyberspace. It will focus on: 1. the thievery of intelligence and information from government and the military, 2. the possibility for a severe attack on national infrastructure, and 3. Can military play a leading role in cyberspace in the potential battleground? Though the military is expected to offer response to a cyber attack, in most countries some parts of national infrastructure belongs to the private sector, thus making military approaches less practical or acceptable. Therefore, this is the field which the government's best approach in terms of public-private partnership (PPPs) might be useful to improve the cybersecurity levels.

Session 7

Cybersecurity Futures

Thursday, February 11, 2016

1000h - 1130h

Chairperson

K. Santhanam

Shri K. Santhanam was the Director General of IDSA during the period 2001 to 2004. He superannuated from the Defence Research and Development Organisation as Chief Advisor (Technology). He was Scientific Advisor in the Ministry of External Affairs and a member of the National Security Advisory Board. He was conferred Padma Bhusan award in recognition of contributions to the Shakti-98 series of nuclear tests conducted in Pokhran in May 1998. He is a co-author of two books *Jihadis in Jammu and Kashmir: A Portrait Gallery* (Sage, 2003) and *Iraq War 2003: Rise of the New Unilateralism* (Ane Books, 2003). His works include *Asian Security and China*, 2000-2010 (Shipra, 2004) and *India and Central Asia: Advancing the Common Interest* (Anamaya, 2004).

TOBBY SIMON

Tobby Simon is the President of Synergia Foundation, a think tank that works closely with industry, polity and academia to establish leading edge practices through applied research in the domains of geo politics, risk management and security analysis.

He has been a speaker at various global public policy conferences, including: World Trade Organization - Geneva, Global Public Policy of the World Information Technology and Services Alliance, Massachusetts Institute of Technology, John F Kennedy School of Government, Council for Foreign Relations, Indian Institute of Management, Indian Institute of Science, the Herzliya Conference and the National Institute of Advanced Studies.

He is currently pursuing his Ph.D. on International Security at the National Institute of Advanced Studies and is a Special Professor at the School of Management in the University of Nottingham.

CYBERSECURITY FUTURES

Tobby Simon

"*Hidden in the dark underbelly of the Trojan Horse, Odysseus and this Greek warriors proved to be the undoing of Troy. Will the World Wide Web and its anonymous residents prove to be the Achilles heel of the Cyberspace*"

The capacity to produce, communicate and use information is affecting every aspect of human security, from the way we govern ourselves (e- government) to the way we fight wars (information warfare), to the way transnational criminal organisations optimise their bandwidth, to the way activist and extremist mobilise support seamlessly across borders.

The geography of Cyberspace is more mutable than other environments. Mountains and oceans are hard to move, but significant parts of the Cyberspace can be turned on and off with the click of a switch. Low barriers of entry contribute to diffusion of power both in the geo-political space and cyber domain. It will be easier and cheaper to move electrons across globe than aircraft carriers thus creating new choke points.

Cybersecurity concerns in the future may primarily revolve around traditional and non traditional areas like health care, consumer devices built on IOT's, hybrid warfare , access to governmental information and cyber weapons by outside organisations or a breach in nuclear or space security .

Sico van der Meer

Sico van der Meer is a Research Fellow at the Netherlands Institute of International Affairs ‘Clingendael’. His research is focussing on non-conventional weapons like Weapons of Mass Destruction and cyber weapons from a strategic policy perspective. He graduated from the Radboud University Nijmegen in 1999 with a Master’s in History. Before joining the Clingendael Institute he worked as a journalist and as a Fellow of a think tank on civil-military relations. Currently he is also a member of the Editorial Boards of the journals ‘Internationale Spectator’ and ‘Security and Human Rights’.

Defence, Deterrence, and Diplomacy: Foreign Policy Instruments to Increase Future Cybersecurity

Sico van der Meer

Predicting the future is hardly possible, but stating that cyber aggression - be it espionage, sabotage or even warfare - will be a continuing threat to international security and stability in the coming years seems a safe forecast. What foreign policy instruments do states have to increase international cybersecurity.

Defence and deterrence, which could be labelled passive deterrence and active deterrence as well, are probably the most 'simple' counter-measures to international cyber aggression that a state could implement. The paper especially analyses why defence and deterrence look like promising policies, but in practice face many difficulties in the cyber realm. Defence and deterrence are not able to create long-term cyber security and stability, but may instead even create further escalation and uncertainties.

Diplomatic efforts to create international accepted norms and rules regarding cyber aggression could be more effective in actively addressing the core problems of international cyber aggression, but are little successful so far. The paper argues that such multilateral diplomatic efforts are crucial to come to long-term cyber security and stability. Instead of an on-going 'cyber arms race', efforts could better be focussed on building mutual confidence and respect.

John Ellis

John Ellis is Chief Strategist - Cyber Security (Asia Pacific & Japan) at Akamai Technologies. An experienced thought leader with more than 20 years of IT security strategy and technology solutions experience, with the last last ten years in spent in Asia. John has held senior technology positions in Standard Chartered Bank, Barclays Capital and Telstra. John is responsible for providing thought leadership and advocating Akamai's security technologies to help customers address their business problems in cyber security.

Disruptive Technologies and the Trusted Cyber Future

John Ellis

Erosion in the trust of digital technology and services continues through the daily news of successful cyber attacks, data breaches, and overt government mass surveillance. Consumers demand convenience and a ‘frictionless’ digital experience, yet expect that their data, money, investments are well protected and privacy respected.

Analysts predict that the world economy stands to lose 3 Trillion USD should we continue ‘muddling' through this problem. With the backdrop of regional and global geopolitical issues, pending crypto-wars, and increasing regulation, what can governments and organizations do to establish trust in their digital economies and business?

The paper also seeks to answer the following questions. What are the top 5 mega trends in disruptive technologies? How will it impact our economies? What are the challenges they present for privacy and trust, and what are the opportunities that they will create? What approaches can governments and industries take to overcome fear in these disruptive technologies so as to build trust and confidence for consumers and industries alike? Is it possible for us to achieve a secure cyber future for all? What are the characteristics of a trusted cyber world? What practical steps can governments and industry take to build a trusted cyber future?

Jonathan Reiber

Jonathan Reiber is a Senior Fellow and writer at Berkeley's Center for Long-Term Cybersecurity. He focuses his research and writing on cyber resilience, national contingency planning, and international security.

Prior to his appointment at Berkeley, he held a number of positions in the Obama Administration within the U.S. Department of Defense. From January 2013 to September 2015, he served as Chief Strategy Officer for Cyber Policy in the Office of the Secretary of Defense. As Chief Strategy Officer, he advised the Pentagon leadership and led strategic initiatives across the cyber policy portfolio, to include strategic planning; key international, interagency, and industry partnerships; and strategic communications. He was the principal author of *The Department of Defense Cyber Strategy (2015)*. In addition to serving as Chief Strategy Officer, he was also the Executive Secretary of the Defense Science Board Task Force on Cyber Deterrence.

Earlier in the Obama Administration, He served as Special Assistant and Speechwriter to the United States' Deputy Secretary of Defense, Dr. Ashton B. Carter, and previously as Special Assistant to the United States' Principal Deputy Under Secretary of Defense for Policy, Dr. James N. Miller. In both positions he focused on strategy, Middle East security, Asia-Pacific security, cyber policy, and public communications.

He is a graduate of Middlebury College, where he studied Religion, and The Fletcher School of Law and Diplomacy, where he focused his studies on international security and U.S. diplomatic history and served as Editor-in-Chief of The Fletcher Forum of World Affairs.

Cybersecurity Futures and the U.S.-India Strategic Partnership

Jonathan Reiber

Following Prime Minister Modi's announcement of Start-up India last week, and using Berkeley's emerging cyber scenarios as a basis, the paper will propose that the U.S. and India should take the next step in their strategic partnership by expanding their cybersecurity cooperation to better account for strategic issues and public-private exchanges. While President Obama has made the U.S.-India strategic partnership a centerpiece of his Administration's foreign policy, despite the escalating cyber threat the two countries have yet to collaborate in depth on strategic issues in cybersecurity. This is a missed opportunity. Using Start-up India as a hook, the paper will look at future scenarios of IT and cybersecurity, and argue persuasively that the U.S. and India can take practical steps together to secure their interests in cyberspace and protect their future economic prosperity. Cooperation should include concrete measures in technology sector collaboration, strategy development, and contingency planning.

Session 8

Panel Discussion: On the Way Forward

Thursday, February 11, 2016

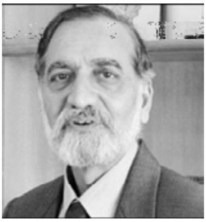
1200h - 1400h

Chairperson

GULSHAN RAI

Dr. Gulshan Rai is the National Cyber Security Coordinator, Government of India. Dr. Rai has over 25 years of experience in different areas of Information Technology which include Cyber Security, e-Governance, Legal Framework and the Information Technology Act for e-commerce, and several related fields. His previous assignments include Director General, CERT-In (Indian Computer Emergency Response Team), Director General, STQC Directorate (Standardization, Testing & Quality Certification) and Head of Department of E-Security and Cyber Law Division in the Ministry of Communications and Information Technology.

Kiran Karnik



Shri Kiran Karnik was the President of NASSCOM, a premiere trade body and the "chamber of commerce" for the IT software and services industry in India, till January 2008. Prior to joining NASSCOM in 2001, he was the Managing Director and CEO of Discovery Networks in India where he spearheaded the launch of Discovery Channel in South Asia in August 1995 and Animal Planet (a Discovery - BBC joint venture) in 1999. From 1991 to 1995, Shri Karnik was Founder-Director of the Consortium for Educational Communication, which was responsible for UGC's Countrywide Classroom broadcasts and other ICT initiatives.

Earlier, he worked for over 20 years at the Indian Space Research Organization (ISRO), where he held various positions including that of Founder-Director of ISRO's Development and Educational Communicational Unit. His work in ISRO involved conceptualizing and managing applications of space technology. He has served as Special Assistant to the Secretary-General of UNISPACE 82 in the United Nations. He has done consulting assignments for WHO, The World Bank, UN Institute for Disarmament Research, Ford Foundation, and an extended one for UNESCO in Afghanistan.

He has been a member of many key government committees, and is presently a member of the Scientific Advisory Council to Prime Minister. He also has a deep involvement with a number of NGOs in the areas of education and environment, and currently is honorary Chairman of the National Foundation of India, Chairman of Vigyan Prasar and President of India Habitat Centre. He has been awarded the Padma Shri in 2007 and the 'DATAQUEST IT Person of the Year - 2005'. A post-graduate from Indian Institute of Management, Ahmedabad, Shri Karnik holds an Honours degree in Physics from Bombay University.

N Balakrishnan

Prof. N Balakrishnan was part of an Expert Group constituted by the Ministry of Home Affairs on "Roadmap for Effectively Tackling Cyber Crimes in the Country". The Expert Group submitted the report on September 2015. Prof. Balakrishnan was the Chairman of Data Security Council of India (DSCI) from August 30, 2010 to 31st March, 2015. Currently He is a Professor at the Department of Aerospace Engineering and at the Supercomputer Education and Research Centre, Indian Institute of Science (IISc). His areas of research include Numerical Electromagnetics, High Performance Computing and Networks, Polarimetric Radars and Aerospace Electronic Systems, Information Security, Digital Library and Speech Processing. He has more than 200 publications to his credit in international journals and international conferences and reports. He was awarded with Padmashree, which he received from the President of India in 2002.

Prof. Balakrishnan is very active in many major Indian and international initiatives in IT planning and information security. He is also Visiting Professor at the Institute for Software Research International, Carnegie Mellon University in the U.S. He is a Fellow of all the major science and engineering academies in India and also a Fellow of TWAS, the third world academy of sciences. He continues to be on DSCI Board as Independent Director.

Santosh Jha

Shri Santosh Jha joined the Indian Foreign Service in 1993. From 1995 to 2004, he served as Second Secretary (Political) in Moscow, was Consul General of India Vladivostok, and later posted to the Indian Consulate in New York, where he handled Press and Consular Affairs.

From 2004 to 2007, he served at the Ministry of External Affairs in New Delhi in the Americas Division where he was involved with India-US nuclear negotiations and also handled issues pertaining to Space, Defence and High Technology cooperation with the USA.

From 2007 to 2010, he was posted to Colombo as Counsellor in-charge of Economic, Commercial and Development Aid issues. He was a member of the Indian delegation for negotiation of the Comprehensive Economic Partnership Agreement (CEPA) with Sri Lanka. After the end of the civil conflict in Sri Lanka in 2009, he was also involved with developing the architecture of development aid from India to Sri Lanka.

From 2010 to 2013, he served as the Deputy Chief of Mission to the Indian Mission to the European Union, Belgium and Luxembourg. During this period, he also served as Charge d'Affaires from January to September 2012.

From June 2013 till 15 April 2015, he was Joint Secretary in-charge of Establishment, Administration and the Europe West Divisions in the Ministry of External Affairs (MEA). Since 15 April 2015, he is serving as the Joint Secretary dealing with Policy Planning, Research and Global Cyber Issues.

Ammar Jaffri

Please refer Pg. 24 for detailed profile.

Gillane Allam

Please refer Pg. 52 for detailed profile.

Greg Austin

Please refer Pg. 28 for detailed profile.

CONTACTS

Name	Office	Mobile
Cherian Samuel Conference Coordinator	91-11-26717983 Extn: 7221	9810809336
Munish Sharma Conference Team	91-11-26717983 Extn: 7335	9916344044
Arul R Conference Team	91-11-26717983 Extn: 7228	9013350392
Ameeta Narang **Sumit Singh** Conference Cell	91-11-26717983 Extn: 7202	9871844607 9999402933
Aparna Krishna Manager, Communications & Outreach	91-11-26717983 Ext. 7204	9899802660
Rahul Gupta Assistant Estate Manager	91-11-26717983 Ext. 7312	8800145788
Gopal Awasthi Assistant Estate Manager	91-11-26717983 Ext. 7305	9899933960
Accommodation IDSA Guest House Shri Nirdosh Tirkey	91-11-26146656 Intercom: 9000	9810890685

asian
security
conference
2016

Securing Cyberspace: Asian and
International Perspectives

Institute for Defence Studies and Analyses
No. 1, Development Enclave, Rao Tula Ram Marg
New Delhi - 110 010
Tel.: 91-11-2671-7983 Fax: 91-11-2615-4191
E-mail: contact.idsa@nic.in Website: http://www.idsa.in