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

asian
security
conference
2016
Securing Cyberspace: Asian and
International Perspectives

RAPPORTEURS REPORTS
&
KEYNOTE ADDRESSES

Securing Cyberspace : Asian and International Perspectives
February 9-11, 2016

The Asian Security Conference (ASC) is a major calendar event of the Institute for Defence Studies and Analyses (IDSA), New Delhi. Since 1999, when the conference was first held, the ASC has emerged as an important platform for debating issues relating to Asian Security. The eighteenth conference in this series was held on the topic "Securing Cyberspace: Asian and International Perspectives".

The Conference consisted of 8 sessions with the following themes:

Session 1: The Global Cybersecurity Environment
Session 2: International and Regional Responses to issues in Cybersecurity
Session 3: Non-State Actors and Cyberspace
Session 4: Securing Strategic Critical Infrastructure
Session 5: Cybersecurity and the Digital Economy
Session 6: Role of Military in Cybersecurity
Session 7: Disruptive Technologies and Cybersecurity
Session 8: Cybersecurity- The Way Forward

Rapporteurers reported on each of these sessions, drawing out the main points and the discussions that followed.

Session 1 : The Global Cybersecurity Environment

18th Asian Security Conference
Securing Cyberspace: Asian and International Perspectives
February 09 - 11, 2016

Chairperson : Nitin Desai

Ammar Jaffri	Varun Sahni	Greg Austin	Cuihong Cai	Yasuaki Hashimoto

The first session of the conference was chaired by former Under Secretary General in the United Nations, Mr. Nitin Desai. . The session focused on understanding the complexity of the global cyber security environment. Ammar Jaffri, Varun Sahni, Greg Austin, Cuihong Cai and Yasuaki Hashimoto presented their views.

Ammar Jaffri

Ammar Jaffri spoke on **Cyber Security Challenges and Opportunities in the Fast Changing World Today**. Ammar Jaffri is the President of Pakistan Information Security Association. ". In his presentation he delved on: 1) use of cyber space in Asian countries…future trends and opportunities, 2) use of cyber space by criminals and terrorist organisations, 3) how to remain secure in cyber space...challenges and solutions, 4) need for regional cooperation for securing the cyber space, 5) use of the internet in the development sector (health, education, etc.) and 6) need for regional cooperation (e-SAARC as a case study). He spoke of the internet as the fastest change in human history, with mankind increasingly dependent on it. He emphasized the fact that

improvement of technological trends and crime has a historical linkage. Due to advanced technology being in the hands of criminals with their own secure networks, the ability to harm has radically increased. The initial success of cyber criminals has encouraged terrorists to use cyberspace.

Jaffri stressed on the need to have a global infrastructure under Interpol to fight various types of cyber threats worldwide. Due to improvements in battle-readiness, especially in the context of Information Warfare (IW), there are multiple attackers and few defenders i.e., lack of manpower in this field. Targets chosen by attackers can have vast tangible value, creating panic among the masses. In this context, he spoke of a possible Cyber Pearl Harbour. Also, with increasing threat of cyber warfare on a daily basis, the governments cannot face the challenges alone. Jaffri had the following suggestions for being prepared for a cyber attack: 1) Research and Development (R&D) 2) systemic improvements 3) cooperation at regional and international level and 4) public-private partnership. He further emphasised the need for creating a web of trust between cyber security professionals.

Varun Sahni

The second speaker of the session was Varun Sahni. He spoke on **Cyber Redefinitions and the Challenged State: Security Implications**. Varun Sahni is a Professor in International Politics at Jawaharlal Nehru University, New Delhi. Prof Sahni started his presentation by speaking on Information, Communication and Technology (ICT) redefining the human and social possibilities, and argued that the traditional notion of state sovereignty is challenged in cyberspace. He agreed on the definition of cyberspace by Martin Libicki which states that Cyberspace as a sum of the globe's communication links and computation nodes. However he was of the view that the territoriality factor was missing in the definition. He argued that the first redefinition of cyberspace pertains to people. The second redefinition of cyberspace was argued to be spatial. Thus he pointed out that cyberspace must be seen in territorial terms. The third redefinition of cyberspace was argued to be about power. Cyberspace augments the capabilities of the government but also provides insurgents with new ways to challenge the established power. The fourth and final redefinition was argued to be sovereignty or exclusive jurisdiction.

He summed up by mentioning that the four classical elements of statehood- population, territory, government and sovereignty have been challenged in cyberspace. He argued that the challenges if not addressed become existential threats and cyber war could be inevitable.

He provided with a fact from the 2013 UNIDIR report according to which 12 states have been found capable of conducting offensive cyber warfare. Thus he concluded by saying that cyberspace has been more securitised than the outer space. The speaker lastly mentioned on the absence of a common understanding on applicable international rules for state behaviour in cyberspace and the problem of attributability in cyberspace.

Greg Austin

The third speaker of the session was Dr Greg Austin who spoke on **Middle Powers and Cyber-Enabled Warfare: The Imperative of Collective Security**. Greg Austin is a Professional Fellow at the East West Institute in New York. The paper focused on national security in cyberspace which according the speaker was much broader and important than cybersecurity. He argued that the U.S. is the only Super Power in cyberspace and mentioned that India and Australia are Middle Powers with respect to the Super Power. He started his presentation by raising the question: will the cost/benefit relationship in technical development and use of cyber weapons change in 10-20 year time-frame? He disagreed with the notion of calling cyber warfare as the fifth domain of warfare; rather, he viewed cyber warfare as being the most lethal of all warfare. He mentioned three layers of a cyber-enabled war – physical, logical and personal. He also discussed eight vectors of attack and defence, i.e., software, hardware, network, payload, power supply, people, policy and ecosystem. Like all wars, political, economic, social and military elements are critical to achieve a political goal. The speaker drew a time-line comparison between U.S. and China on the development of cyber capabilities. Austin spoke of four key aspects in terms of the future trends of cyber enabled war- 1) political goals, 2) multi vector, multi- front, multi- theatre, 3) sustained, cyber and kinetic, 4) resilience, 5) advanced situational awareness and 6) scenario planning.

With respect to critical infrastructure, he mentioned that intrusion detection technology is not well developed enough for control systems network. He also pointed to the fact that even an "air-gapped" ystem could be breached. He argued that Middle Powers needed to augment their situational awareness system, which currently does not exist with most Middle Powers. He questioned on how much a Middle Power could spend to protect itself from high profile cyber-enabled warfare. Hence he proposed for the single option of collective security by the States. Austin pressed for middle powers to develop complex responsive systems of decision making for medium intensity war that address- 1) simultaneous multi- vector, multi- front and multi- theatre attacks in cyber space by a determined enemy and 2) including against civilian infrastructure and civilians involved in the war effort. In conclusion, he spoke of building a community of interests around the concepts of cyber enabled warfare and war avoidance with States collectively including U.S. and China that would bring together all the available expertise

Cuihong Cai

Cuihong Cai, addressed the theme **'Global Security Environment: Perspectives of the US and China in Comparison.'** She divided her presentation into four parts: 1) concepts; 2) reconstitution of security problem into network problem; 3) common global security techniques; and 4) differences between US-China. Dr Cai highlighted the prevailing issues in global cybersecurity environment, namely information inundation, information pollution, information infringement, information monopoly and cybersecurity crisis.

The speaker further elaborated that cyberspace can be used for power games between nation-states, leading to conflict and control of security practices. Moreover, all actors in the cyberspace have capacity to launch attacks and there is no concept of geography in the networked environment. She pressed on the need of differentiating between combatant and non-combatant entities in cyber space.

The speaker brought in the subjectivity in the understanding of security environment, elaborating how the US views it from the prism of "threats", while China defines the cybersecurity environment from the perspective of development. The threat-based approach defines it from the perspective of ""others", and the development-based approach focuses more on "own" needs, to enhance the development and security of cyberspace. Speaking on network filtering and monitoring techniques, Dr. Cai highlighted that the social and political stability is regarded as the primary national cyberspace interest for China. According to her, difference in understanding of core cybersecurity interests between China and the US results in their different cognitions about the cybersecurity environment as well as deficiency of the mutual trust in the cyberspace.

Yasuaki Hashimoto

The fifth and the final speaker of the session was Mr. Yasuaki Hashimoto who spoke on the theme **'Present Situation of Japanese Cyber Security'**. He began with the rising number of cyber attacks in Japan. Japan faces Distributed Denial of Service (DDoS) attacks and Advanced Persistent Threat (APT) led attacks, targeted at leading companies in aerospace industries, the Diet (national parliament) and Japanese diplomatic offices abroad. Responding to such threats, the Japanese Government had established Cyber Security Strategy in 2013. Subsequently, in 2014, the Japanese Diet passed the Cyber Security Basic Law, under which National Center of Incident Readiness and Strategy for Cybersecurity (NISC) in the cabinet office is headquarters of the national cyber security practices. The Cyber Security Basic Law respects the rights of the citizens including freedom of information, while maintaining cyber security. The Japanese Ministry of Defence (MoD) also has its own Cyber Defence Unit since 2014; however, this unit only protects the networks owned and operated by Ministry of Defence and does not cover the whole national cyber network infrastructure.

The speaker highlighted that the Cyber Security Strategy was revised in September 2015, and it recognizes cyber threats as a critical challenge to the national security. Prof. Hashimoto touched upon the Japanese support for international cooperation and its participation at various bilateral and multilateral platforms such as Convention on Cybercrime, Japan-U.S. Cyber Dialogue, Japan-US Defence Cooperation and Japan-ASEAN Cybersecurity Policy Meeting.

Discussions

There were many interesting questions from the floor during the discussion dealing with the non-awareness of an upcoming cyber attack, technical comparison of cyber warfare with WMDs, possibility of an international treaty on cyberspace, successful case studies of good cyber partnerships between states, the role of diplomacy in cyber- space and the role of cooperation between states.The panel responded to many of these questions with creative analysis. The possibility of deterrence in cyber space being difficult and the threats involved in cyber space are more was pointed out by Dr Cai. In terms of successful partnerships between states in dealing with cyber space, she gave the example of China- Korea, China-UK, China-ASEAN, China-SCO etc. Dr Austin pointed out that the role of diplomacy in cyber space is very complicated and it is resilience to attacks that gives a country national and international credibility. Also, he stressed that there will always be news ways to attack; the states need to learn to adjust with the technological changes. Mr. Jaffri pressed for Confidence

Building Measures (CBMs) to deal with the issue of mistrust between states. He emphasised the role INTERPOL can play in the matter of cyber security. People to people contact, was the other strong emphasis made by Mr. Jaffri. In the discussions, Mr. Hashimoto raised the issue of cyberspace being multi-layered leading to discarding of the use of traditional means to understand cyberspace. Prof Sahni spoke of supra- state structures being provoked and playing a significant role in cyber security. He further pointed out that the components of state have shifted.

Session 2: International and Regional Responses to Cybersecurity Challenges

Chairperson : Latha Reddy

Alexandra Kulikova	Nandkumar Saravade	Candice Tran Dai	Munish Sharma	Cherian Samuel

Session 2 on "International and Regional Responses to Issues in Cybersecurity" was chaired by Latha Reddy, former Deputy National Security Advisor (Deputy NSA). She referred to the IDSA's Task Force Report titled *India's Cyber Security Challenge* published in 2012, which had many useful inputs and had been considered by the Government of India while formulating the National Cyber Security Policy (NCSP). She said that the basic framework for a cyber security policy is now in place for the Indian government. The policy is being implemented through the creation of various mechanisms and institutions including a Joint Working Group (JWG) on public-private partnership, and the creation of the post of NCS Coordinator. Praising the continuing efforts on cyber security, Latha Reddy requested the first speaker, Alexandra Kulikova, to speak on "Working out the Rules of Global Cyberspace Governance".

Alexandra Kulikova

Alexandra Kulikova spoke on the topic **Working out the rules of Global Cyberspace Governance**. Kulikova is the Global Stakeholder Engagement Manager for Eastern Europe and Central Asia at ICANN. She talked about the state reaction to Cybersecurity challenges, in particular about norms building and Confidence Building Measures (CBMs) with a view to

create trust among states. The speaker pointed out that the recent cyber-attacks proves that this technology could be lethal and could wreak havoc. However, diplomatic efforts have been concentrated on cyber-conflict regulation but not on prevention of conflict. She mentioned about the Tallinn manual, which is a type of regulation on how international law is applied to cyber-conflicts. She commented that the Russian Government has been involved in the area beyond cyber-conflict since the late 1990s through UN Group of Government Experts (GGEs). The speaker presented the variety of approaches in norm building in cybersecurity as there are differences in approaches and methods to the concept "norm" itself. The Shanghai Cooperation Organisation (SCO)'s Code of Conduct for Information Security, 2011 looks at protecting information space, in particular the sovereignty of a state. She pointed out that the Western countries obviously disagree with this approach as they see it as a move to increase state control over the information space. However, the speaker pointed out that the 2015 text is better as it talks about CBMs.

The other forms where the issued was raised included the Convention of International Information Society, Ekaterinburg in 2011 and the Global Conference of Cyberspace (GCCS), London in 2011. She brought to attention the contribution of private companies with their own recommendations of the norms, which included norms for restraining weaponising cyberspace. The speaker argued the GCCS in Hague did not show much progress on norms building, in particular the possibility of a treaty. It did however bring together stakeholders from different arena, not limiting to just state actors. She also mentioned John Kerry's speech in Seoul and successive UNGGE reports. She highlighted that the Report of the 2015 UNGEE was voluntary and not binding, but its existence is significant and a good starting point for further build-up of norms. Russia found it encouraging that the document mentions state sovereignty as well as the ideas from SCO Code of Conduct. She expressed the hope that the CBMs and capacity-building measures along with norms can build a global cyber security ecosystem. She suggested that the UNGGE is still an inspiration to regional and bilateral initiatives and an opportunity for cross-fertilisation of ideas. The Organisation for Security and Cooperation in Europe (OSCE) conference on cyber security in 2013 adopted CBMs and is another platform to talk about cyber security and the stumbling blocks. The BRICS is also active on the issue of cyberspace as they have common denominations, even though the constituent states are focussing on their own agenda. There are also ongoing bilateral discussions, such as between US andRussia, US and China and China and Russia. The US-Russia cyber security agreement in 2013 is promising, even though it has been temporarily frozen due to the situation in Ukraine.

The China-US communique of 2015 shows that both countries are giving importance to cyber security. She concluded that norm-building creates an ecosystem and trust between states and complements all the other developments regarding cybersecurity, and a multi-stakeholder approach is crucial for its implementation. In fact, pacing and timing is crucial, and smaller, quicker and more rational initiatives are required.

Nandkumar Saravade

The next speaker Nandkumar Saravade spoke on '**International and Regional Responses to Cybersecurity Challenges**'. Saravade is the CEO of Data Security Council of India (DSCI). The speaker emphasised that unlike other nuclear and chemical threats between nation states, cybersecurity is different and might not be amenable to the similar approaches. The recent developments in cyberspace have created both enthusiasm and apprehension. The Internet of Things and Big Data Analytics, though quite useful technologies yet pose greater security challenges in cyberspace. He was also of the view that Artificial Intelligence should not be developed. The rapid advance of technology has its advantages for businesses and government to support economic growth but will also continue to present challenges. Due to the advance in Internet connectivity in the world, there will be the generation of the data leading to complexity in the world. The speaker pointed out that due to these changes, now organisations are investing in location-based services, behavioural advertising and Wearable Information Technology. According to the speaker, this would result in highly invasive technologies whereby a whole gamut of personal data will be generated and consumed by the service providers. This would also affect business ethics regarding Big Data and private sectors have themselves admitted to be not fully prepared to handle these Big Data challenges. The speaker stressed that the range of actors and attacks have increased and critical infrastructure is now more vulnerable. He gave an example of a kinetic attack that happened in a Eastern European country which affected its critical infrastructure (Electricity Grid). Unlike state actors, where deterrence could be exercised, in cyberspace, the same is not possible with the ability and the agility of non-state actors. In his view, cyberspace is much more offense-dominated where the attacker always has more control of the situation. Therefore, cybersecurity requires multiple conventions, frameworks and stakeholders to solve these issues. However, although states use a lot of approaches such as laws, information sharing mechanism and involving corporates to secure cyberspace, many countries are unable to counter the cybersecurity challenges. Regional initiatives in Asia such as ASEAN initiative such as the Singapore Declaration has been noteworthy for providing a platform for the integrating countries in combating cyber-crime, terrorism and transnational crime. He mentioned on the role of ITU, NATO and other international bodies in Europe and concluded that the UNGGE was so far the most successful forum where agreement was made on basic cybersecurity problems. He was of the view that that it was the responsibility of the State to protect the critical-infrastructure of the country and secure it from malicious attacks. In this regard, international cybercrime investigation and collaboration needs a closer look. The current multilateral assistance mechanisms such as the Mutual Legal Assistance Treaty are not working efficiently as it takes a lot of time to receive information. He concluded by stressing on the development of standards and frameworks in the pace as the technologies grow.

Candice Tran Dai

Candice Tran Dai, the next speaker, spoke on **'Economic Dimensions of National Cybersecurity Strategies in the Asia-Pacific Region'**. Candice Tran Dai, spoke on "Economic Dimensions of National Cybersecurity Strategies in the Asia-Pacific Region". She first referred to the evolution of the cyber security policy, which systematically integrates economic dimensions such as national security, innovation capability, and commercial interests. France has voted for a sovereign operating system, which is an indigenous cyber technology capacity. South Korea has specified the target countries for domestically-made cyber security exports. Both these measures have economic dimensions. She noted that while cyber security is about securing cyberspace, it is also a business and a market evolving into an industry. She stressed that the economic dimensions of a cyber security strategy are growing visibly. Asian countries are integrating the economic dimension into cyberspace, which could be termed as ambition or industrial policy. Economic dimensions in India's cyber security policy are very pragmatic, so that economic interests are protected to provide opportunities for innovation to domestic industries. China on the other hand, has been consistently focusing on promoting the domestic information security industry and expanding the discourse on indigenous innovation. Japan has revamped its cyber security strategy in 2013 and in the final draft in 2015, it has highlighted the economic dimensions of cyber security. South Korea also has strong ambition to export domestically developed cyber security products and information security. These initiatives show that states have been integrating economic dimensions in their cybersecurity policies and are linked to their quest for enhancing indigenous cybersecurity capabilities. This shows a desire for domestic innovation with regard to ICT technology, to be freed from dependency on foreign ICT technology, especially US cybersecurity products. This strategy is preferred because indigenous ICT technology is safer and controllable with potential market access for foreign vendors. Therefore, cyber security should be looked through the global cyber security supply chain and international trade perspective. An example of this is seen in the Free Trade Agreements (FTA), especially in Trans-Pacific Partnership (TPP) negotiations whereby, among 30 chapters, three chapters are devoted to cyber security. Other avenues include the World Trade Organisation (WTO) and the Wassenaar Arrangement. The Wassenaar Arangement's additional items on cyber security would be subject to export controls and will affect businesses. This would compel states to balance cyber security export ambitions and their commitment to the Wassenaar Arrangement. Finally, she concluded that cyber security is subject to tradeoffs between national security and international trade.

Munish Sharma and Cherian Samuel

Munish Sharma and Cherian Samuel were the last speakers on the topic "**A South Asian Regional Cybersecurity Cooperation (SARCC) Forum: Prospects and Challenges"** Munish Sharma is an Associate Fellow with cybersecurity project in IDSA. Cherian Samuel is an Associate Fellow in the Strategic Technologies Centre at IDSA. They speakers spoke on the paper titled A South Asian Regional Cybersecurity Cooperation (SARCC) Forum: Prospects and Challenges. They mooted the idea of a cybersecurity cooperation within the regional organisation of SAARC. They stressed that almost all countries in SAARC post 2003 has strengthened their cybersecurity institutions and laws by creating CERTs (Computer Emergency Response Teams) and enacting acts and designing cybersecurity strategies. A SWOT analysis of the SAARC cybersecurity forum was discussed in detail. The idea of a SAARC CERT was proposed. The speakers concluded on the note that 21st century should set an example with cyber-diplomacy making the way for greater regional cooperation in the field of cybersecurity.

Session 3 : Non-State Actors and Cyberspace

18th Asian Security Conference
Securing Cyberspace: Asian and International Perspectives
February 09 - 11, 2016
asian security conference 2016
idsa

Chairperson : Ravi Kant

Alok Vijayant	Sanjeev Relia	Arun Mohan Sukumar	Gillane Allam

Mr. Ravi Kant in his opening remarks underscored the growing importance of cyberspace for nation-states and highlighted the vulnerabilities, to which, these Critical Information and Infrastructure systems (CII) are subjected. He held that the anonymity provided by cyber space with little risk of attribution, has provided nations an option to employ non-state actors to achieve their limited strategic goals, without inviting any political risk. As a result, the nation-states have less incentive to support a legally binding definition of cyber warfare, which would, otherwise, limit their freedom of action in cyberspace. Hence, in the current decade, non-state actors have become a reality in the cyberspace with which nation-states have to grapple.

Alok Vijayant

The first speaker was Mr. Alok Vijayant. He spoke on the topic of **Asymmetrism in Cyberspace: State vs Non-state Actors**. Cyberspace was the fifth domain of warfare, where national boundaries, individuals and states do not matter. Asymmetrism in cyberspace alters the nature of war; for non-state actors to wage a war against nation states, they do not need large infrastructure, and the battlefield is distributed. An investment in a laptop, internet connection and a skilled logical brain is sufficient for non-state actors to initiate war. Describing the characteristics of cyber warfare, Mr. Vijayant held that the war in cyberspace has become borderless with 'no identifiable centre of gravity'; with non-State actors employing unethical weapons to target their enemies such as use of False Flags, religious leaders and theology for subversion of institutions of learning and culture.

According to the speaker, the community of hackers, comprised of both organised and unorganized segments, is one ecosystem, while the executive and legislature of a nation state form another ecosystem, and both have no interaction. Due to this disconnect, it is challenging to frame laws, rules and regulations for the community of unorganized hackers. Discussing the case of Wassenaar Arrangement as a weapons control regime, the speaker argued that deterrence is the only way to control cyber weapons and defy the non-state actors from indulging in the acts of belligerence, because it is extremely difficult to identify a cyber weapon at the first place, as it may reside on a laptop or a mobile or simply on a pen drive. He stressed on the need to convert Black Hat hackers into White Hat, and maintain the right balance between offence and defence.

Sanjeev Relia

The second speaker was Sanjeev Relia. His topic was **Non State Actors and Cyberspace: An Overview.** He highlighted the threats posed by non-State actors in the virtual world (cyber) and held them as much perilous as the threats posed by non-State actors in the real world. However, in the absence of any universal classification, there are two broad categories into which non-state actors could be divided; a) organizations who have created or who manage cyberspace; and b) the actors who pose threats. Such non-state actors could be part of radical groupings with their own ideological, political or religious reasons. They have not carried out any major attack in cyberspace, but they exploit it for recruitment, funds or propaganda. The other set of non-state actors, the cyber militia are volunteers who can work on behalf of a nation state in order to achieve a political goal. Cyber militia have advantages of their own ; they need not be based in the same country which gives them the freedom to attack from anywhere, their operations are cost effective, and it protects the attacker nation state from any political ramification, so there is low risk of a counterstrike because there is no attribution. The speaker discussed the case of Unit 61398 of the Peoples Liberation Army (PLA) of China. The unit is a classical example of Cyber militia, focused on a military objective and given the clandestine nature of its operations; China denies the very existence of any such unit.

Articulating the threat from cyber militia to India, the speaker stressed on the fact that 8.31 percent systems in India were found to be infected with Stuxnet virus, as per the analysis report of Symantec. A nation state, or someone on the behest of a nation state can sabotage the critical information infrastructure, be it telecom banking or power. The speaker argued that, given the advantages of cyber militia, these non-state actors are most suited cyber adversaries during peace time. As India embarks on digitization, subversion of human and systems, espionage operations on citizens and soldiers are the most prominent threats.

Arun Mohan Sukumar

The third speaker was Mr. Arun Mohan Sukumar. He spoke on **State and Non-State: Residual Actors in Cyberspace**. He focused on three main aspects; a) whether non-state actors could be regulated; b) application of international law on non-state actors and; c)non-state actors with agency. On non-State actors in cyberspace, the speaker argued that the international regime in cyberspace treats NSA as residual actors; rather they are“non-State actors with agency” and not the“proxies of nation-State”.

Reflecting on the desirability to regulate such non-state actors, Mr. Sukumar noted that there are two opposing schools of thought;–One, which is held by the states like China, Pakistan etc., who perceive non-sstate actors in cyberspace as “desirable” to offset the conventional superiority of the adversary by engaging the latter in limited warfare. The opposing school of thought is governed by the state’s rational as to whether the cost of “reputational loss” of engaging such non-state actors in cyberspace exceeds over the benefits they accrue by harbouring them as an unregulated force.

Speaking on the absence of international norms regulating non-state actors in armed conflict, he cited UNGGWE principles where, international law applies to the acts of states in cyberspace and states should do all they can to prevent injurious acts from their territories. Highlighting the issues in case of armed conflicts, primarily attribution and conduct of non-state actors during conflict, Mr. Sukumar concluded his presentation by asserting the need to recognise non-state actors in cyberspace as “non-State actors with agency”, they have a mind of their own, they are not necessarily extension of state or proxy of the state.

Gillane Allam

The last speaker of the session was Amb. Gillane Allam. Amb. Allam provided an insightful geopolitical and geostrategic understanding of non-state actors as perceived by the states of North Africa and West Asia, speaking on "**Non-State Actors & Cyberspace - A North African Perspective**". She took an historical account of the events which led to the evolution of non-state actors in West Asia since the early 1980s. The withdrawal of Soviet armed forces from Afghanistan and thrust on "Political Islam" gave rise to many non-State actors like Al-Qaida, Taliban, Hamas and Hezbollah.

The speaker discussed the case of Daesh in detail, its modus operandi and cyberspace strategy, which is often accredited as effective and professional. Cyberspace is central to its organisational activities, namely, garnering financial support, recruitment of foreign fighters, radicalization, trainings, ideology and propaganda dissemination, communication with the world, or to glorify the acts of terror.

Amb. Allam concluded that violent, extremist and armed non state actors should be totally contained and possibly eliminated. Therefore, Cyberspsace should be monitored and positively directed through internationally agreed upon instruments. In addition to the international military campaigns against terrorism, there is a pressing need at the international level as well to wage a committed digital counter insurgency campaign. According to the speaker, the possible solutions could be fair sustained development, social justice, promoting greater tolerance within and between nations and deepening understanding between religions.

A pertinent point emerged during the discussion, the threat of non-state actors in cyberspace can be countered by building mutual trust and developing confidence within the states. Hence, the states should share the forensic details of cyber attacks with each other, and accordingly, the cases can be forwarded to neutral organisations like INTERPOL for investigation.

Session 4 : Securing Strategic Critical Infrastructure

idsa
INSTITUTE FOR DEFENCE STUDIES & ANALYSES
Celebrating 50
asian security conference 2016
18th Asian Security Conference
Securing Cyberspace: Asian and International Perspectives
February 09 - 11, 2016
Kah-Kin Ho
Jana Robinson
Alhad G Apte
Caroline Baylon
A Vinod Kumar

Chairperson : Alhad G Apte

Ted G. Lewis	Kah-Kin Ho	Jana Robinson	Caroline Baylon	Vinod Kumar

Ted G Lewis

The first speaker Ted G Lewis presented via Skype on the topic **Challenges of Cybersecurity: Malware and AS-level Structure.** He flagged the policy and technical challenges of cyber security. Among the former included the issue of cooperation across all levels of government, IT skills lacking in government, issues relating to civil liberties as a result of government regulations, among others. As for technical challenges, Dr. Lewis pointed out that the language of the internet – TCP/IP, was never designed to be secure. He noted the evolving nature of the threat from malware, the convergence of the internet with other critical sectors like water and transportation, the prevalence of ‘weak edges’ (weak authentication capabilities in platforms like cell phones and laptops), among others. Dr. Lewis noted that the ‘resilience’ of the internet could be increased by reducing its vulnerabilities at critical points, the so-called ‘blocking nodes’. Hardening a small percentage of such nodes will reduce the vulnerability. He also called for the development of the capability to detect malware at these nodes. Responding to questions, Dr. Lewis pointed out that the randomization of routing structures will make the network more robust and that the problem of anonymity could be solved by using ‘time-stamps’. He however pointed out that the TCP/IP does not support ‘time-stamps’.

Kah-Kin Ho

Kah-Kin Ho, Head of Strategic Security, CISCO who spoke on the topic **Evolving Role of Government in Critical Infrastructure Protection**, pointed out that most of the critical infrastructure in Europe and the United States was being run by the private sector. He noted that 'security incidents' have a crippling and cascading effect. Mr. Ho put forward a framework which could capture the changing role of the government as a provider of security. This was 'Regulate' (government setting the terms and conditions), 'Facilitate' (helping the private sector do its job better) and 'Collaborate' (in partnership with the private sector). Mr. Ho noted that the private sector has 'next level considerations' which prevent it from investing effectively in cyber security solutions. These considerations include the fact that there are many risk factors for a private sector company, issues pertaining to budget and overall security culture, the belief that security measures do not make a difference anyway, 'fear mongering' (statements like there are only two kinds of companies – ones that have been hacked and ones that do not know they have been hacked), among others. Factors that could induce greater private sector investment on cyber security include market forces, 'lead dog' entities (major companies that lead by example), among others. He urged for the adoption of an offensive mind-set by critical infrastructure providers to better anticipate adversarial moves. He noted that while 'regulations' are useful, they will only work effectively in a 'high-trust' environment.

Jana Robinson

Jana Robinson, Space Security Program Director at the Prague Security Studies Institute (PSSI), spoke on the topic **Governance Challenges at the Interaction of Space and Cybersecurity**, pointed out that cyber-related vulnerability of space assets was an increasing concern. She called for increasing public-private partnership to address cyber threats to space operations effectively. She pointed out the need to consolidate the command of space and cyber space domains, given that configuring adequate defences for both military and civilian operations are challenging. Ms. Robinson also dwelt on the great power politics inherent in efforts to come to

a common understanding on the threats posed to outer space. She noted that Russia and China, which were at the forefront of efforts at promoting arms control in space domain, had several differing views on security concepts with the European Union for instance on the Code of Conduct for Outer Space. She urged for transparency and confidence-building mechanisms (TCBM's) as well as clear procedures on escalatory spirals and other eventualities for mature crisis management architecture.

Caroline Baylon

Caroline Baylon, Director of the cyber security research program at the Centre for Strategic Decision Research in Paris spoke on the topic **Cybersecurity Threats to Critical Infrastructure: A case study of Nuclear Facilities.** She noted the increased availability of automated tool kits which can detect critical infrastructure connected to the internet, making them vulnerable to possible attacks. While nuclear facilities are relatively secure as compared to power grids for instance, she however noted that nuclear facilities are increasingly adopting features that make them vulnerable digitally. These include the use of the internet by third-party entities like crisis responders requiring access to data, vendors that need to remotely monitor their equipment, among others. She noted that the nuclear industry was increasingly transitioning to digital without fully understanding the risks. Among industry-wide challenges she pointed out the insufficient spending on cyber security and the greater vulnerability of developing countries, especially their lack of access to current best practices. Ms. Baylon further pointed out that cultural difference between IT engineers and Operations Technology engineers for instance (with the latter preferring safety over security) accentuates cyber risks. Technical challenges associate with the nuclear industry included dated industrial control systems without in-built authorisation or encryption features.

Vinod Kumar

Vinod Kumar, Associate Fellow, IDSA spoke on the topic **Securing Critical Infrastructure from Cyber Threats: Developing Defence, Deterrence, and Norms.** He noted that attribution and retaliation continued to pose a problem in the arena of cyber security. He pointed out that critical national infrastructure (CNI) was fast emerging as the new zone of conflict, with the energy sector being the most vulnerable, along with the finance and the military sectors. While the nuclear sector was getting the more public attention, in his opinion, it was not as vulnerable as the other CNI. He pointed out the incompatibilities between the concepts of nuclear deterrence and cyber deterrence, including regarding such concepts as attribution, the issue of 'rational actors', and 'pre-emption' among others. While 'deterrence by denial' could be ensured through strong defences in the cyber domain, there was a need for clear declaratory policies by nation states to ensure 'deterrence by retaliation'. He termed as 'oxymoronic' the use of such terms like 'ethical hacker'.

Session 5: Cybersecurity and the Digital Economy

idsa
INSTITUTE FOR DEFENCE STUDIES & ANALYSES
Celebrating 50
asian security conference 2016
18th Asian Security Conference
Securing Cyberspace: Asian and International Perspectives
February 09 - 11, 2016
Uchenna Jerome Orji
Madan M Oberoi
V K Saraswat
Liam Nevill
I L Seok OH

Chairperson : V. K. Saraswat

IL Seok OH	Liam Nevill	Madan M. Oberoi	Uchenna Jerome Orji

The session was chaired by former Director General of the DRDO, and current Niti Aayog member, Dr. V.K Saraswat. The chairman made a few introductory remarks, noting the importance of digital technologies to both the civilian sector and the military.

IL Seok OH

The first speaker, IL Seok OH, from Republic of Korea gave a presentation on **Korean Legal Initiatives to combat Cybercrimes and enhance Digital Economy**. He began by outlining the extent of the cyber attacks faced by South Korea, giving specific examples. The South Korean nuclear power plant operator, Korea Hydro and Nuclear Power (KHNP) was breached on December 2014, resulting in the leak of personal details of 10,000 KHNP workers, designs and manuals for at least two reactors, electro flow charts and estimates of radiation exposure among local

residents. In similar vein, cybercrimes in the form of Phishing, SMS Phishing, Memory Hacking and Palming are on rise in South Korea. The estimated loss due to cybercrimes has amounted to $ 4.8 billion annually, prompting the government to consider cyber security as the one of main factors to enhancing national security. Cyber security was emphasised in the National Security Strategy 2014, The government designated a Special Secretary of Cyber Security in Blue House in January 2015. Moreover, the government has enacted various legislations namely Electronic Financial Transaction Act, Cyber Security Industry Enhancement Act, Act on Promotion of Information and Communications Network Utilization and Information Protection and the Personal Information Protection Act.

Liam Nevill

Liam Nevill gave a perspective on **"Challenging opportunities for the Asia-Pacific's digital economy"**. The three key points of the presentation is that in order to unlock the potential of the digital economy in Asia-Pacific lack of connectivity, lack of trust and lack of regulatory framework needs to be addressed. Asia-Pacific is a heterogeneous region when it comes to digital infrastructure and capacities with some of the most advanced to the least developed, and the most connected to the least connected countries. The limited ability of many states to invest in adequate infrastructure to harness the potential of the digital economy remains an impediment to growth. In the Asia Pacific, about 8 per cent of the population has access to fixed broadband services, and these are often financially out of reach to lower income populations. However there may be benefits in bypassing the development of fixed infrastructure. Mobile phones have provided online access to a new generation in the region, and growth has been considerable. The diversity of markets and levels of development mean that there is no 'one size fits all' solution to the challenges that face further digital economic growth. Similarly, issues related to cybercrime and cyber security leads to lack of trust and a major impediment to adoption of digital technologies. Without a reliable and safe cyber environment, business will hesitate to invest in new business markets and models. The World Economic Forum estimates that if national and multilateral cybersecurity efforts are not effectively implemented and cyber criminals retain their advantage, up to USD$1.02 trillion in the value of the global digital economy would not be achieved. Conducive regulatory and tax frameworks will encourage investment and innovation in digital economy and boost start-ups in the field of e-commerce.

Madan M. Oberoi

Madan M. Oberoi, Director, Cyber Innovation & Outreach, INTERPOL gave a law enforcements perspective in his presentation titled "**New Technologies and New forms of Crime**". The recent trends in technology have led to multifold increase in devices connected which has exacerbated insecurity in mind of the users. Cybercriminals have used technology to commit financial crimes like ATM manipulation, Bitcoin extortion and money laundering through crypto-currency. Internet has been used by extremist for online radicalisation. Dark Net has been used to market and sell illicit goods online, the online drug website Silk Road being the most famous instance. Cybercriminals offer their services to conduct crimes like Bitcoin theft, theft of computational resources for mining bitcoin and unleashing Ransomware. The collusion of new technologies and cybercriminals has led to new challenges for law enforcement agencies. Such challenges needs a recalibration of law enforcement strategy and shift has to be towards a multi-stakeholder model involving private sector, academia, research bodies, Inter-Governmental bodies, Civil Society and law enforcement agencies.

Uchenna Jerome Orji

The African perspective was presented by Uchenna Jerome Orji titled **"Regionalizing Cybersecurity Governance in Africa: An Assessment of Responses"**. Africa has witnessed phenomenal growth in Internet Communication Technology (ICT). The penetration of ICT's has led to increase in cybercrimes and general digital insecurity. To address these concerns, several African intergovernmental organizations have developed legal frameworks to promote the regional governance of cybersecurity and also facilitate the harmonisation of cybersecurity laws in Member States. 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. However, given the global nature of the Internet, regional cybersecurity governance arrangements would never be able to replace a widely accepted global cybersecurity governance arrangement. Nevertheless, regional arrangements may provide platforms for building global consensus on cybersecurity governance. Despite their jurisdictional limitations regional governance arrangements hold prospects towards facilitating legal harmonization and promoting cooperation to the widest possible extent among Member States.

Session 6: Role of Military in Cybersecurity

Chairperson : Prakash Menon

Liina Areng	Amit Sharma	Caitriona Heinl	Li-Ching Yuan

The Chairperson for the session, Lt. Gen. Prakash Menon, introduced the thematic framework for the session by stating that cyber security, in essence, means the 'security of information', and hoping that the papers will elucidate and examine the general principles that determine the military's role in cyberspace.

Liina Areng

Liina Areng, speaking on the **Role of Military in Cybersecurity** started with an overview of the attributes of the digital landscape that defines her country, Estonia. Being known as one of the most 'wired' countries of the world, she described the contours of Estonia's digital economy where 95 % taxes are filed online 98 % of patients access e-medicine and over 90 % of kids gains benefits of e-schooling. Estonia enrols over 60 million digital signatures every year and has started e-voting since 2005. Areng explained the significance of Estonia's digital way of life, which protects its national values through information and communication technologies (ICT). Estonia has both the advantage and disadvantages of being a small state, with one of the gains of its digital power being the short reaction time to crises.

Areng underlines critical strategic infrastructure as a strategic game-changer in cyberspace, and explained how the Black Energy Trojan attack on a Ukrainian CNI facility as examples of vulnerability of this domain. Areng differed with earlier presentations about the invalidity of Mutual Assured Destruction (MAD) in cyber affairs by affirming that it remains relevant to this space with a reconfiguration of Mutual Assured Doubt, where uncertainty will be the key. Areng emphasized that much of cyber talent is not in the military domain. During a crisis, a shifting of duties and roles from CERTs to military teams may not be a feasible proposition – implying that cyber attacks and resultant crises should be dealt with consolidated teams. Areng highlighted the need to build international cooperation through collective brain pools, exercising and a strong community – as intended through models like the NATO Cooperative Cyber Defence Centre of Excellence.

Amit Sharma

In his presentation titled **The Triad Theory of Cyber Warfare: A Framework for Strategic Cyber Warfare,** Amit Sharma attempted to provide a new framework of cyber defence, deterrence and offensive strategies. Sharma began with the affirmation that cyber is generally reflected upon as a revolution in military affairs (RMA), followed with a 'strategic effect'. He questions whether cyber has any strategic effect, though it juxtaposes various principles of both Clausewitz and Sun Tsu. Sharma points out that informationisation adds to the vulnerability of nations and makes it what could be termed as a 'risk society' where the cascade effect of cyber attacks could lead to strategic paralysis.

Sharma outlines a campaign plan for a broad cyber warfare strategy, spread into three phases: pre-conflict, conflict and post-conflict phases. In the first stage, Sharma argued, vulnerabilities should be introduced into the enemy system, hitting critical links (underwater cables and satellite links), through a triad system. He listed the triad as included: (a) Triad 1 – civilian and military cyber capabilities, (b) Triad 2 – 'air-gapped' systems, and (c) Triad 3 – Cyber Militias. Sharma premises this stage to be of a 'countervailing strategy' where the adversary is signaled of capabilities and intentions in order to make deterrence credible. The second phase – of conflict – is when deterrence fails and when a state has to take down the cyber deterrence capabilities of the rival's triads. The third phase – post-conflict – is of an exit strategy, where the emphasis will be to not expose oneself to the rival militias. In Sharma's perception, the pre-conflict is current on in cyberspace. He concluded with the affirmation that a cyber defence framework will include layers of technology, legal instruments and pure cyber deterrence.

Caitriona Heinl

The presentation by Caitriona Heinl on **International Military Cyber Cooperation in Asia** largely examined the national and regional cyber cooperation frameworks in the Asian region, with specific reference to military cyber cooperation. Heinl insisted that many national cyber policies do not match and prioritize regional cyber frameworks which in turn affect cooperation. The primary reason for this situation, she feels, is the divergent threat perceptions of states, along with the lack of trust and transparency. Heinl contends that pragmatic military measures should be taken in conjunction with the visions of political leaderships on how cyber cooperation frameworks have to evolve at the regional level. And for this to be effective, military institutions have to be involved in cyber dialogues.

Heinl felt that India has an active cyber diplomacy strategy, as is visible from the various initiatives taken by the Indian government. While emphasizing on the importance of regional cooperation to ensure stability in cyberspace, Heinl pointed to the India-Japan-Singapore-Malaysia Memorandum of Understanding (MoU) on cyber cooperation as a unique regional model. At the same time, she cautioned about skepticism that the defence communities in the Asian region generally have towards cyber confidence building measures (CBMs). In this direction, Heinl argued that hotlines should be included between national cyber institutions and officials in order to improve CBMs.

Li-Ching Yuan

Li-Ching Yuan started the last presentation in this session on the topic **Role of Military in Cyberspace: Case of Republic of China (Taiwan)** with an analogy that while water can carry boats, it could also capsize them, indicating the opportunities and threats in cyberspace. He warned that cyber systems of a nation are targeted when there is heavy reliance on such infrastructure. Yuan explained the national cyber security architecture developed by Taiwan, including the various monitoring and cyber defence agencies that function under the National Security Bureau, which is the final frontier against all cyber threats. Yuan gave a SWOT analysis of Taiwan's cyber security apparatus by listing a vibrant ICT industry and direct supervision of the section by the information and security office of the Union Cabinet as among Taiwan's biggest strengths, while pointing to lower awareness of users and weak defences against hackers, along with not-so-active international cooperation as among their key weaknesses.

Yuan identified the scope for greater investment in information security mechanisms as an opportunity while listing Chinese hackers as the greatest threat, including the claim that Taiwan is test bed for Chinese PLA cyber unit 61398. He went on to list statistics to impress upon the high instances of cyber attacks on Taiwan. To counter this, Taiwan has established the Information and Electronic Warfare Command under the Ministry of National Defence. Yet, he felt that Taiwan's cyber warfare capabilities remain insufficient and its assets vulnerable to various threats. Yuan mentioned that a National Information and Community Security Task Force have been constituted with the objectives of protection, investigation and defence of critical national infrastructure. He indicated that military cannot be deployed in Taiwan's domestic cyber affairs due to legal and regulatory issues, and also because the cyber command is under strict political control.

While summarising the presentations and debate, Lt. Gen. Menon, highlighted two significant aspects. First, despite the many strategies of defence, offence and deterrence being articulated by experts in this session, including of cyber militias, no nation can impose their strategic writ or objectives by using cyber capabilities – be it weapons or proxies. He warned that like in the conventional realm where nations could retaliate when subjected to an attack or conflict, the same kind of repercussions could be expected even when offences are planned in cyberspace. Second, he felt that cyberspace, despite being a common space of all nations and individuals, continue to be remain in anarchy, thanks to the absence of norms and order.

Session 7 : Cybersecurity Futures

Empowering People
idsa
INSTITUTE FOR DEFENCE STUDIES & ANALYSES
18th Asian Security Conference
Securing Cyberspace: Asian and International Per
February 09 - 11, 2016
Jonathan Reiber
Rumel Dahiya
Tobby Simon
Sico van der Meer

Chairperson : Brig. Rumel Dahiya (Retd)

Tobby Simon	John Ellis	Sico van der Meer	Jonathan Reiber

Tobby Simon

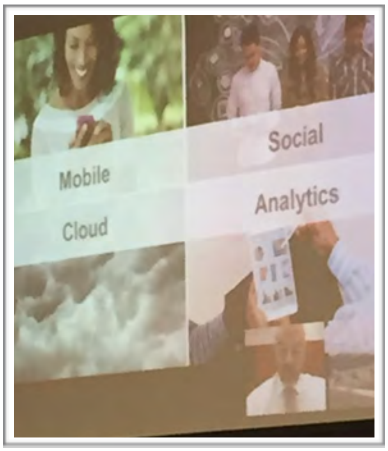
Session 7 was chaired by Brig. Rumble Dahiya (Retd), Deputy Director General, IDSA. The first speaker was Tobby Simon. He spoke on **Cybersecurity Futures**. Tobby Simon spoke on "Cybersecurity Futures". His presentation focused on Botnets, Encryption, IoTs (Internet of Things), Supply Chain Security, ICS and Supervisory Control and Data Acquisition (SCADA), Space Security and Cyber Terrorism. He mentioned that Cyber security is not a technical problem but a military one. He mentioned that the role of government is a big one in the future. In his presentation, Tobby Simon characterised cyber threats as akin to a war of attrition through the use of a large number of tools varying from sophisticated worms to botnets. These vectors can be used for a variety of actions, from gaining control of missiles (GPS) to manipulating social media (through twitter

bots, etc.). Sophisticated worms can be made to lie dormant for years and activated at vulnerable times, such as during a national disaster. With the speed of quantum computing any encryption can be broken, thus laying waste the backbone of cyber security. What will happen if a big company like Infosys is attacked and the attack becomes public? The answer according to N.R. Narayana Murthy is that it will be the beginning of the end for the Indian computing industry.

However, the fact remains that cyber is not so much a technology problem as it is a human intelligence issue. The human is the weakest link in cyber security. Thus, there is a need for more security management of people, people who understand security issues. The role of the government is also set to increase since citizens will turn to the government in case of a security issue rather than to companies.

John Ellis

The second presenter was John Ellis whose presentation was via Skype. He spoke on **Disruptive Technologies and the Trusted Cyber Future**. He averred that Over the Top (OTT) Services like WhatsApp, Facebook will dominate in the future. In his presentation, John Ellis emphasised that the importance of internet to business is huge as almost all business depends on internet. Whole sectors have been disrupted because of cyberspace and the trend is set to continue. By 2020, it is estimated that more people will watch video online than on TV. This has also made cyberspace attractive for criminals. 575 billion $ is the cost of cyber-attacks annually. By 2019, cyber-attack risks will lead to an added 35 per cent expenditure on security.



Security by design is essential in cyber business and important to keep systems free of vulnerabilities. Many governments lack the necessary means to protect citizen data and information. Therefore, more stringent laws and many financial penalties will be seen applied in the short term. Building a trusted cyber world is necessary. And this requires concerted and coordinated actions by governments and companies. Governments, industries and business create a sense of conflict for the user since the user has varying demands and requirements from each of them.

It is necessary to change the economics in favour of the defender, to build capacity to recover faster from attacks, and to make it harder for the adversary to initiate an attack. This includes undertaking user training as humans are the first line of defence in cyber-attack. He mentioned four ways to build a trusted cyber world. They are Digital resilience, Digital Trust, Cost to the adversary and Collaboration. Integrated and a holistic approach is needed for the future of cybersecurity.

Sico van der Meer

The next speaker was Sico van der Meer. He spoke on **Defence, Deterrence and Diplomacy: Foreign Policy Instruments to Increase Future Cybersecurity**. Sico van der Meer. He spoke on “Defence, Deterrence and Diplomacy: Foreign Policy Instruments to Increase Future Cybersecurity”. The speakerHe preferred to use the term “Cyber-Aggressions”. More and more states are getting engaged in cyber deterrence but this is a short- term solution. Deterrence by denial is complex and expensive. Deterrence by DenialIt is also passive deterrence. In the cyber world, your opponent will always be ahead of you. The human is always the weakest link in cyber domain. The other deterrence is deterrence by retaliation through the use of sanctions, etc. The problem of attribution is a big major problem in deterrence by retaliation. Good cyber- forensics and conventional intelligence is a pre-requisite for a good cyber attribution. The speakerHe was of the view that both deterrence by retaliation and denial will only escalate things and is are not a good options. The speaker proposesHe proposed that diplomacy would be a long- term and best solution to handle cyber- aggressions. Building global norms and values would be the initial step in thefor long- term diplomatic actions.

Jonathan Reiber

Jonathan Reiber. spoke on **Cybersecurity Futures and the US-India Strategic Partnership**. How can increased resilience be built in societies so that they can bounce back after an attack? States and companies are extremely vulnerable to cyber attacks. The US is 90 per cent penetrated by cyber technologies and thus the range of cyber attacks is huge. The Department of Defense (DoD) has to safeguard its networks otherwise the military cannot undertake its functions. The DoD works closely with the FBI to counter threats emanating from cyber attacks. The US follows the doctrine of restraint where breaking the internet is not an option. Cyber attacks are more likely to happen during a conflict or during negotiations. The US military will look for ways to undertake cyber attacks in order to prevent loss of life.

US-India collaboration could be improved in the following ways. The three areas that need to be focused on are technology sector collaboration, strategy development and contingency planning. Encryption, norms and state behaviour are areas that also could be focused on. He mentioned that Cyber defence was not dealt with in the India-US Cyber dialogue of September 2015. He concluded by emphasising strengthening of the Public-Private Partnership (PPP) for countering threats..

Session 8: Way Forward

Chairperson : Gulshan Rai

Prof. N. Balakrishnan	Lt Gen Aditya Singh	Shri Santosh Jha	Prof. Greg Austin	Shri Ammar Jaffri	Amb. Gillane Allam

The last session of the 18th Asian Security Conference on "Securing Cyberspace: Asian and International Perspectives" was chaired by Dr Gulshan Rai, National Cyber Security Coordinator, Government of India. There were six panelists: Prof. N. Balakrishnan, Amb. Gillane Allam, Lt Gen Aditya Singh, Shri Santosh Jha, Prof. Greg Austin, and Shri Ammar Jaffri who deliberated upon the main ideas that had emerged during the two-and-a-half day conference and provided key recommendations for addressing the various threats emanating from cyberspace. The following is a summary of the discussion

IT proliferation is growing and the application of the internet is increasing with mind-boggling speed. The internet has become a very reliable mode of communication. It helps pass information relating to any activity including academia, business, defence, or anything that one can talk about. Many new technologies have emerged in the last ten years. When social media emerged in 2005 nobody had imagined it will have such a penetration, affecting every aspect of human life. Mobile technology has also made a revolutionary impact on day-to-day life. It was pointed out that while technologies and their uses are growing rapidly, these pose new challenges as well– in the form of security of the assets and of the information contained in those assets. These have brought new paradigms in the areas of cyberspace security and management, as cyberspace has transcended national boundaries. Thus, while the commercial use of the internet has increased exponentially, maintaining net neutrality remains an important challenge and a debatable concept. Consequently, security and privacy has become more important today. A great deal of confusion prevails however, over this because the technologies have not been distinguished between civil and military. Things are becoming more converged and diffused as the same technologies can be used both for civil and military purposes.

Cyber space is used both for development and mass destruction. In the meantime, the digital empowerment has become an unavoidable choice for all. The emerging cyber challenges are common to the international community and sometimes there can be specific challenges to a region or country. It was stated that the rapid expansion of the use of cyberspace by people will further increase pressure on the government for maintaining balance between national security and freedom to use cyber space.

Moreover, with the deep penetration of social media in today's life, cyber space-instigated violence and atrocities in the real space are the biggest problems. The nature of challenges coming from cyber space has rapidly changed from web defacement and password stealing to stealing of industrial information and secrets. Now, information security and cyber space security means different things to different people. While a corporate would want to secure the network and the information, the government and people would want to secure something different from cyber threats. It was believed that cyber media-instigated terrorism will probably be the biggest security threat to nation-states in the coming years. For instance, ISIS is regularly using this for recruitment. A lone wolf terrorist actually uses this to pass his message. The lessons and techniques that have been learnt so far must be used to predict and defend before any such attack occurs. Furthermore, in India, the differences between the print media, electronic media and the internet were not properly understood. While the print and electronic media message goes off in a short time, the information shared through the internet via social media such as WhatsApp, Twitter, stay for a long time. Hence, there are ways and means to monitor social media messages and the threats emanating from this can be prevented through active intervention.

However, a big challenge is attribution of cyber space violation. It becomes more acute and complicated when different actors such as non-state, proxy, and anonymous, are involved. There are also differences between countries, especially in the way they see cyber space activities. So, developing regional and global partnerships is very important for addressing this growing challenge. Public and private diplomacy can play a key role in building such partnerships.

At the same time, no one is denying the great advantages it has brought to the people. Speaking on the subject, Lt Gen Aditya Singh provided a very optimistic view by saying, "the world is [a] much better place today than five years ago, and it will be a much better place five years ahead." Recalling the horrors of the 20th century's world wars where millions of people died, he said, it is unthinkable today. Whether it were the smallpox or swine flu viruses, the world has overcome those challenges. The world is now beginning to cope with new challenges such as the Ebola or Zika viruses and surely will resolve them sooner or later. He stressed that the benefits of cyber space will far outweigh the pitfalls and the world will learn to deal with the pitfalls. One of the ways is to do this by spreading the awareness. The national and international dialogue over this issue has increased recently which contributes to spreading cyber awareness. This debate and discussion will further contribute to develop cooperation among nation-states to address the prevailing pitfalls. In this regard, the first step forward is CBMs.

INSTITUTE FOR DEFENCE STUDIES & ANALYSES
18th Asian Sec
Securing Cyberspace: Asian
February
Santosh Jha
Aditya Singh

Since people live in a world of cyber ambiguity, it was suggested that a statement of doctrines or policies by countries can create confidence. For instance, there is no definition of cyber terrorism in the world today. If nations can come together on a common definition then cooperation can be developed on this. Another way to go forward is through bilateral dialogue and cooperation. Since multilateral negotiations sometimes become difficult to address the dyads of challenges that a country faces, multilateral fora may be used for broader areas of cooperation. Prioritising cyber threats will also be crucial in going forward as the threat comes in different forms. The effect of cyber on strategic stability should be regarded as the topmost priority where it can do maximum damage. This aspect can be brought forward for dialogue and developing cooperation between countries. Major events on cyber space can also be used as a forum for cooperation. Though there may not be a permanent solution to this problem as the world continues to evolve, the countries can have a multi-pronged approach to deal with this challenge.

Meanwhile, cyber diplomacy has acquired a new prominence in India's bilateral and multilateral engagements. It remains at the top of the list as India's aspiration to play a leadership role in shaping the global agenda has increased in recent years. As a result, cyber dialogue and cooperation has been emerging as one of India's important engagements. Importantly, India supports the multi-stakeholder model for internet governance. In this context, the role of the state has become paramount in addressing the cyber challenge because it is the state that ultimately has to implement policies.

Additionally, India is making efforts to address the global cyber problem by enhancing bilateral and multilateral partnership and cooperation at the multilateral fora. It has developed cyber security partnerships with a number of countries and will soon forge a partnership with China as well. In these partnerships, the focus has been to build confidence by information-sharing, capacity-building, and R&D in the cyber security arena. India as the second largest internet user is now poised to play a larger role in the cyber domain.

Importantly, the international discourse on cyber space is positively evolving, and the panelists underlined the significance of cyber norm development. It was stressed that restraining and controlling behaviour in the arena of cyberspace would help enhance cooperation among countries. Greater transparency and accountability on internet governance will further help in building such norms. However, the emergence of two camps – one led by the US and the other by Russia and China – remains a big challenge in developing international cooperation on internet governance.

Another big challenge that remains to be addressed is the security dilemma over cyber space. Though a cyber-enabled war between two countries seems very unlikely in the immediate future, it could create strategic instability by affecting the nuclear command and control system of a country. Therefore, it was suggested that setting up cyber hotlines between nations would help address the misunderstandings that prevails over cyber space-related activities and help reduce existing threat perceptions in critical security areas. It was also suggested that establishing an International Cyber Security Centre would be more useful, as the prevailing international norms and multilateral fora on cyber space are not affective in addressing the cyber security challenges.

Most of the panelists underscored the significance of public and private partnerships in addressing the emerging cyber space challenges, as the government alone cannot. It was believed that the private sector can substantially contribute to build cyber infrastructures. They also highlighted the importance of R&D, capability building, information sharing and awareness on cyber space. Moreover, a cyber space partnership between government, university, civil society and technology partners can be developed in this area. The partnership should first start at the country level, then at regional level and finally at the global level for building confidence to counter the challenge. However, building greater synergy between national and international partners, defining and interpreting privacy, attribution of cyber violation, and defining international legal frameworks for jurisdiction, will be critical for effectively addressing cyber issues and managing them in the future.

Keynote Address by Air Marshall PP Reddy VM, ADC - 9,February, 2016

Dr Jayant Prasad, Director General IDSA

Distinguished guests and participants,

Ladies and gentlemen,

1. It gives me great pleasure in welcoming you all to the 18th edition of the Asian Security Conference. Since its inception in January 1999, this Conference has served as a forum for free and open discussion by security analysts, experts and scholars from different parts of the world. The theme of the 18th Asian Security Conference – 'Securing Cyberspace : Asian and International Perspectives' is a highly relevant and extremely contemporary as cyberspace has become an arena for co-operation, competition as well as conflict.

2. The traditional bases of national power have included the economy, military capabilities, the science and technology base, and national resources including physical resources, human resources, infrastructure, and knowledge resources. The arrival of the Information Age is widely seen as a momentous development, as revolutionary as the Industrial Age, with information processing regimes replacing manufacturing as the source of wealth and growth. Cyber and information technologies have added a new dimension to the various components of national power, creating both new capabilities as well as new sources of vulnerabilities. Cyberspace and cyber technologies today, have become key components in the formulating and execution of national policy. Cyber technologies are also entwined across the key components of national power and act as a force multiplier, thereby creating new synergies and unleashing new forces, sometimes with disruptive effects.

3. The Prime Minister of India, while enunciating his vision of a Digital India conceptualised an India "where government services are easily and efficiently available on mobile devices; where government actively engages with people on social media; where mobile phones enable personal services; and where cyber security becomes an integral part of the national security." Towards this end, the Govt of India has started a number of programmes to leverage information technology for the benefit of citizens. The "Digital India" and "Smart Cities" are flagship programmes with a vision to transform India into a digitally empowered society and knowledge economy. Another flagship programme of the Government of India is "Make in India" which is designed to facilitate investment, foster innovation, enhance skill development, to

protect intellectual property rights and to build best-in-class manufacturing infrastructure for products made in India. Both the programmes operate by leveraging the use of information technology. It goes without saying that this accelerated capacity building has enormous implications for the country's cyber-security posture.

4. With over 400 million Internet users, whose number is growing rapidly, India has an enormous stake in a safe and secure cyberspace. The Indian government has always stood for an open, global and secure cyberspace and is also aware of the fact that this goal can only be arrived at through international co-operation and collaboration. At the same time, threats from both state and non-state actors, are weakening the very foundations of this concept.

5. As highlighted earlier, cyberspace has today become an intricate constituent of national power having a peaceful as well as the military dimensions. And hence the involvement of the Armed Forces in the domain, in order to secure it, as also to develop credible deterrence capabilities. With militaries adopting network centric warfare and migrating towards more complex Info & Comn systems, they are at elevated risks of cyber attacks. Several nations have documented their cyber strategies and executed them through organisations and structures in the form of Cyber Commands etc, while several other nations are frequently making changes, based on dynamic nature of the envisaged threat. Cyberspace is also witnessing a race for development and deployment of cyber weapons, and has therefore been one of the major security concerns of the Nation States.

6. “Will strategic stability in a globalised and digitised environment be feasible, considering the rapid increase in threats and violations in an unregulated cyber space” is what we all need to sit together and discuss. Are we today witnessing a sort of Cyber Arms Race akin to the nuclear or missile arms race of yesteryears? Can we have international regulatory mechanisms binding on activities in cyber space, and efficacy of such mechanisms on cyber domain where physical inspections etc are of little relevance? Or should regulations be through treaties or conventions or a simple code of conduct by nations, organisations, and individuals?

7. There are also questions about whether existing laws and conventions on war, particularly the Laws of Armed Conflict (LOAC), and International Humanitarian Law can be adapted to the new environment of cyber warfare. The basic principles that have governed definitions and responses to traditional war, such as sovereignty, jurisdiction, use of force, self-defence, proportionality, distinction, and necessity, cannot be easily adapted to cyberwar. Malicious actors, state-sponsored or otherwise, are taking advantage of the confusion to carry out action that come below the thresholds of the definition of war. The question then arises as to which is the appropriate body that would counter or deter such attacks. One of the most difficult issues related to adapting the existing international law to cyberspace is to do with cyber weapons. There is as yet no legally agreed upon definition of a cyber weapon, and the unique characteristics of cyberspace make defining a cyber weapon, that much more harder. And that raises the legitimate question as to whether cyber weapons are a reality, something with which we have to live with and hence devise ways and means to deal with them.

8. Of course, none of these laws apply to the terrorist organisation who have adapted themselves in innovative ways to become one the most ardent users of cyberspace for a variety of purposes, from communication, to finance, as well as for recruitment, networking and psy ops as we are currently witnessing. As the visual and real worlds get increasingly integrated with the Internet of Things (IoT), it is only inevitable that terrorists will try to use cyberspace for destructive purposes as well.

9. With the cyber arena now recognised as a new and distinct domain of warfare, setting up a force competent to achieve the dual objectives of defending the country from cyber attacks in war and securing the military's network operations in peace, requires considerable thought. In the near term, cyber has added a new dimension to the traditional warfare. While both on the ground is not going to be replaced by cyber armies operating in a virtual battlefield in the near future, information dominance in the battlefield may well make the difference between victory and defeat. On the other hand, increasing use of Info & Comn Tech by the armies of today, can also lead to destruction through the manipulation of information by opposing forces.

10. Requisite capabilities for protecting the Indian cyber space, both for civil and military applications, are slowly but steadily, being enhanced. Cooperation amongst the nation-states and a consensus approach, for regulating cyber space need to be adopted by the global community to ensure that the cyber domain is used primarily to enhance quality of life of citizens of our nations, and to strengthen peace, stability and development.

11. In this multi-dimensional, dynamic and evolving medium that we call cyberspace, one finds both, great challenges and great opportunities. I am sure, that the thought and perspectives of the eminent speakers at this conference, including experts and thinkers in cyber technology from around the world, will go a long way in shaping the future of cyberspace and cyber security.

Thank you.

Jai Hind!

idsa
INSTITUTE FOR DEFENCE STUDIES & ANALYSES
रक्षा अध्ययन एवं विश्लेषण संस्थान
Celebrating 50 Years of Objective Research
asian security conference 2016
18th Asian Secu Conference
Securing Cyb pace: Asian a Internationa spectives
Februa 2016

Air Marshall PP Reddy releasing the Asian Security Review Book 2016

Keynote Address by Dr Arvind Gupta, Deputy National Security Advisor - 10,February, 2016

I would like to thank Ambassador Jayant Prasad, Director General of IDSA for inviting me to address the participants of 18th Asian Security Conference. With its eighteenth edition ASC has truly come of age.

2. The theme chosen for this year's conference is apt. The world is becoming increasingly turbulent. The unstoppable march of globalisation, facilitated by ICTs, has raised many troubling questions concerning the maintenance of peace and stability. Cyber security is now an international security concern. It is also a top concern for most countries and figures high in their national security priorities. The focus is on managing the threats in cyberspace which affect everyone. The key question before a state is how to defend itself from the ever increasing occurrences of cyber-attacks.

3. The year 2015 saw a number of important developments in the field of cyber security. President Xi's visit to the US in September 2015 will be remembered for some outspoken public comments by President Obama on US concerns over on-line theft of intellectual property. Aware that cyber concerns, if unresolved, can create misunderstanding and destabilise the bilateral ties, the two countries agreed to bilateral cyber security dialogues. In President Obama's words, the two governments agreed that "neither the US nor the Chinese government will conduct or knowingly support cyber related theft of intellectual property including trade secrets or other confidential business information for commercial advantage". President Obama, according to reports, took up strongly with President Xi the issue of cyber threats. On his part, President Xi, declared that "China strongly opposes and combats the theft of commercial secrets and hacking attacks". The meeting took place in the backdrop of a well-publicised cyber-attack on the Office of Personnel Management (OPM) resulting in the stealing of the fingerprints of 5.6 million people in December 2014 and compromising records of some 22 million people. Acknowledgement by both sides that cyber security is an issue between them was in itself a remarkable development. During the same year, China and Russia also signed a comprehensive agreement on cyber security.

4. In 2015, the UN Group of Governmental Experts (UNGGE) came out with its 3rd Report which was an advance over the previous report. As a result of the efforts of the UNGGE, there is now a growing recognition that international law, particularly the UN charter, applies

as much as to cyberspace as to other domains. The UNGGE emphasises that principles of sovereign equality; settlement of international disputes by peaceful means; refraining from the threat or use of force against the territorial integrity or political independence of any state; respect for human rights and fundamental freedoms including the freedom of expression; and non-intervention in the internal affairs of other states are some of the principles which also apply to the ICT security. In other words, international law is technology neutral. One of the main observations of the report is that states have jurisdiction over the ICT infrastructure located within their territory.

5. The international law has many aspects including intervention in self-defence, economic sanctions, counter measures and so on. A debate has broken out whether intervention through cyber means in other countries' networks, under certain circumstance, is justified or not. The debate is sharp but inconclusive.

6. Cyber security issues are contentious and are proving to be difficult even as the incidents of cyber-attacks, cybercrime, cyber terrorism grow exponentially. Every year new types of attacks are invented and carried out. The toolkit of attackers is expanding. It is quite possible that states may be clandestinely developing arsenal of tools of cyber-attack even as they discuss the need for accepted norms in cyberspace.

7. The challenge before states is how to defend their critical, military and civilian infrastructure from destabilising cyber-attacks. Cybercrime is on the increase. Theft of personal information and intellectual property is rampant. The distinction between state and non-state actors in cyberspace is blurring. Even as technologies of active defence are developed, the attackers are several steps ahead.

8. While most states are engaged in implementing strategies to defend their networks from cyber-attacks, they are also toying with the idea of developing capabilities which would deter potential attackers. Efforts have been made to develop a theory and practice of "cyber deterrence" on the lines of nuclear deterrence.

9. Drawing analogies from the nuclear arms control vocabulary, it is argued that both denial and punishment are essential for deterring cyber aggression. The idea is to make it clear to the potential attacker that the cost of cyber aggression will outweigh the benefits. An effective cyber deterrence strategy will include deterrence by denial as well as penalty by punishment. Deterrence by denial will rely on strong defences. The efforts of the attacker would be rendered futile if defences and resilience i.e. the capability to bounce back are strong. Deterrence by punishment, on the other hand, relies on the ability to counter attack. It is argued that the attacker should know that retaliation should be "certain, severe and immediate". This will deter him.

10. The question is whether cyber deterrence can work in the way similar to nuclear deterrence. Nuclear deterrence works because both sides know fairly accurately the nature, size and scope of each other's nuclear arsenal and the means of delivery. Over decades, arms control negotiations were focussed on issues such as transparency and verifiability of each other's arsenals. Detailed nuclear CBMs, based on verification, were developed. Attempts

were made to understand each other's nuclear doctrines. In the nuclear cease, actors were few. Non-state actors did not possess nuclear weapons. In cyberspace, the situation is vastly different. As yet, there is no clarity even on what cyber-attack means. There is no agreed definition of a cyber- weapon. There are no means of verification. Multiple actors operate in cyberspace with complete anonymity.

11. Sceptics point out that cyber deterrence will fail because of the lack of attributability in cyberspace. In cyberspace, where anonymity is the key, it is difficult to identify precisely who the attacker is. Non-attribution is the fundamental weakness of the cyber deterrence argument. There is, however, some literature which suggests that the problem of attribution may be overcome sooner or later. Such claims are, however, unverifiable at present.

12. For cyber deterrence to be meaningful, a state would have to define its thresholds through appropriate signalling. It will need to indicate its cyber thresholds. Some ambiguity will no doubt be deliberate. Yet, a potential attacker should know that retaliation would be severe and unacceptable if a redline is crossed. Indicating redlines will depend upon a country's capabilities, intents and interests. Today, the redlines are absent. For instance, should cyber espionage, directed against military and non-military targets, be treated as an act of cyber warfare? Is an attack on the banking networks, stock exchanges, power grids an act of war? Does cyber espionage merit a counter attack? Should retaliation be in cyberspace or by other means? With key questions unanswered, to have a cyber-deterrence on the lines of nuclear deterrence seems difficult.

13. The Tallinn Manual 1.0, originally called Tallinn Manual on the International Law applicable to cyber warfare, deals with conflict scenarios in cyberspace where international law would apply. While Tallinn Manual is not an official document, its work is sponsored by NATO and other countries. Presently, a second version of the Tallinn Manual, Tallinn Manual (2.0), is being worked out. The Tallinn Manual 2.0 deals with the application of international law to cyberspace during peacetime. A recent meeting held in the Hague on 2-3 February dealt with these issues. During discussions, attempts were made at defining a diplomatic law for cyberspace. It was suggested that attack on the computer systems of a foreign embassy should be prohibited by law. It was also professed that intervention in cyberspace may be permitted under certain circumstances.

14. In India's point of view, Tallinn Manual, while being a useful exercise, does not reflect the existing law on the subject because of the absence of state practice which is critical for development of customary international law.

15. These difficulties notwithstanding, states are going ahead with incorporation of cyber security in to their military doctrines. Such doctrines postulate that a state, exercising its right to defend itself, could retaliate to a cyber-attack by cyber or any other means. The US national strategy of 2015 says that US could use cyber tools or other means to retaliate against cyber-attacks.

16. The problem of cyber-attacks cannot be seen in isolation. Today, cyberspace is inter-twined with other domains of warfare, namely, land, water, air and space. This inter-twining

implies that cyber-attacks will not be seen as mere cyber-attacks. The retaliation in non-cyber form i.e. retaliation through non cyber means including possibly military means cannot be ruled out. Cyber-attacks, as means of warfare, would only enlarge the battle domain. Cyber warfare may induce states to opt for full-spectrum deterrence.

17. Cyber warfare is a contested concept. Cyber espionage, attack on critical infrastructures etc are routine happenings in cyberspace. So far military means have not been used to deter attacks. Nor have economic sanctions been used because attributing a cyber-attack has been so difficult. Further, many victims feel shy of reporting cyber-attacks. Such incidents have not been regarded as acts of warfare so far because no definition of cyber warfare exists so far. Whether a cyber-attack is seen as a component of cyber warfare will depend upon the context of the attack. The authors of the Tallinn Manual have grappled for many years to come up with some acceptable definitions but so far the progress has been slow.

18. India cannot be oblivious to these developments. Internet usage is spreading rapidly in India. Even though internet penetration in the country is still low, nearly 400 million people are using the internet. Digital India will take broadband internet to every village Panchayat. With one billion SIM card subscribers, a revolution in connectivity is sweeping India. India's future progress and growth is linked with the expansion of the digital network, overcoming digital divides and ensuring that robust cyber security policies are adopted right from the beginning.

19. India has taken several steps in the recent past to strengthen its cyber defensive capabilities. To mention a few:

- A national cyber security policy has been announced and is being implemented.
- An elaborate national cyber security assurance framework is under implementation.
- The National Cyber Security Coordinator appointed last year is coordinating the Indian cyber security effort spread across the various agencies.
- Coordination amongst various agencies has improved.
- A National Critical Information Infrastructure Protection Centre (NCIIPC) has been set up. There is a regular dialogue with the key sectors of the economy.
- Public-private partnership is being constructed. There is an active dialogue between the government and the private sector.
- A National Cyber Coordination Centre (NCCC) is being set up.
- Efforts are being made to develop cyber security skills in the country. New cyber security curricula are being introduced in the colleges.
- Cyber security R&D policy has also been under active consideration of the government.
- CERT-India, an organization that was set up in 2004, has done significant work in dealing with cyber incidents as well as spreading awareness.

- India is pursuing active cyber diplomacy with cyber security dialogues having been set up with several countries and is participating in several international fora including the UN on cyber security.

20. All these synchronized and coordinated efforts are already showing results. But we cannot be complacent in the face of growing threats and evolving technologies. Due to the explosive growth of ICTs, cyber security scenario is likely to remain challenging. We will need to work hard on the various aspects of cyber security including the emerging challenges.

21. Like other countries, India also faces the daunting task of stopping and preventing cyber-attacks on its networks. India will have to closely study the evolution of cyber deterrence idea. Building cyber deterrence capability would entail building robust networks that can be defended, encouraging comprehensive R&D in the area of cyber security and strengthening indigenous manufacture of ICT products and technologies. It will also require strong cyber diplomacy to ensure that India is not at the receiving end of the emerging ICT Export Control regime under the Wassenaar Agreement. We also need to closely analyse the patterns of cyber-attacks against us and build suitable response measures including the capability to conduct cyber operations if required. India would need to take note of the increasingly assertive cyber security doctrines that are being adopted by other countries. This will help in working out our own cyber security doctrines. The inputs from the Conference like this would be most useful.

22. In conclusion, I would like to point out that there is a lack of consensus in the international community on norms of behaviour in cyberspace. We are at a stage where technology is far ahead of our thinking on cyber laws and cyber norms. The UN Group of Governmental Experts has proved to be a useful platform to discuss these issues but the absence of a broader representative platform where contentious issues can be hammered out and consensus arrived at is conspicuous by its absence. Ad-hoc groups adopting ad-hoc procedures to deliberate over ad-hoc cyber security agendas will not necessarily build a consensus. The international community needs to come together to discuss how to deal with threats in cyberspace which are growing by the minute. The task may seem daunting but states should seriously reflect whether the world needs a Cyber Convention on cyber security. Unlike in the other commons like the land, the sea and space, where international law has grown immediately, cyberspace is still largely lawless. This Conference, where leading experts have assembled, can generate ideas on the way forward towards building a consensus on cyber security issues.

Thank you!