INSTITUTE FOR DEFENCE STUDIES & ANALYSES
रक्षा अध्ययन एवं विश्लेषण संस्थान

BIMSTEC

IDSA-BIMSTEC Workshop on Cyber Security Cooperation: A Report

December 05-07, 2018

New Delhi, India

Introduction

Formed in June 1997 in Bangkok, the Bay of Bengal Initiative for Multi-Sectoral Technical and Economic Cooperation (BIMSTEC) has emerged as a key organization for regional cooperation over the last two decades, bridging South and South-East Asia on the prime issues of connectivity, trade and energy. A regional organisation comprising of seven nations from littoral and adjacent areas of the Bay of Bengal, BIMSTEC represents close to 20 percent of the global population and constitutes combined Gross Domestic Product (GDP) of USD 3.5 trillion. BIMSTEC has identified six key sectors (viz. trade and investment, technology, transport and communication, energy, tourism and fisheries) and 14 priority areas, each of which is led by a particular member state.[1] India is the Lead Country for Transport and Communication, Tourism, Environment and Disaster Management, and Counter Terrorism and Transnational Crime sectors. As an economic bloc of developing economies, BIMSTEC Member States face several challenges, which are quite similar in nature and character; be it infrastructure development, natural disasters, radicalisation, terrorism or public health.

With the global advancements in technologies related to information processing, information dissemination, communications, space exploration and others, the issues concerning cybersecurity and peaceful uses of space have gained salience in the overall national security preparedness of the BIMSTEC Member States. Burgeoning economies all, secure cyberspace is essential for the BIMSTEC Member States to harness its true benefits for business development, jobs creation, and technology innovation and also to attract investments.

The BIMSTEC Member States are also continuously subject to a variety of threats emanating in cyberspace from a host of state and non-state actors. The numbers of fraudulent activities in the banking systems have also shown an upward trend – the Bangladesh Bank heist of February 2016 being one of the most sophisticated and serious instances. Combating these threats, which are essentially transnational, requires coordination between the cyber and national security apparatus of the states, their law enforcement agencies, and the respective judicial processes. An effective and co-ordinated collective response requires exchange of information on national strategies and policies; consultative frameworks for confidence building; enhanced information sharing on ICT security incidents; and enhanced mechanisms for law enforcement cooperation.

[1] "About BIMSTEC", at https://bimstec.org/?page_id=189.

It is equally important for the BIMSTEC Member States to learn from the experiences of others and help each other in building their respective capacities and human resources in order to address this rising challenge.

The principles of sovereign equality, territorial integrity, political independence, no-interference in internal affairs, peaceful co-existence and mutual benefit are deeply enshrined in the BIMSTEC approach to cooperation. In line with the Bangkok Declaration, heads of government, ministers and senior officials from BIMSTEC Member States meet regularly at different forums of policy-making and operational bodies. BIMSTEC Summit, Ministerial Meetings and Senior Officials Meeting from foreign and trade and economic affairs are such bodies.[2]

Security is integral to the development and prosperity of BIMSTEC Member States, and in pursuance to the decisions taken at the BIMSTEC Leaders Retreat held in Goa, India, on 16 October 2016, the first meeting of National Security Chiefs of BIMSTEC Member States was hosted by India in New Delhi in March 2017.

This meeting laid the foundation for a collective response to both the traditional and non-traditional security challenges common to the Member States.[3] The Meeting also underscored the emerging trends in cyberspace that have security implications, and decided to establish a Joint Forum to strengthen cyber security among the BIMSTEC member states. At the Second Meeting of the BIMSTEC National Security Chiefs, held in August 2018, India proposed a three day workshop on cyber security for the BIMSTEC Member States.

Subsequently, the Institute for Defence Studies and Analyses and the National Security Council Secretarial held a three day workshop* on cyber security from 05-07 December, 2018 at New Delhi. The first two days of the workshop involved presentations, deliberations and discussions on national perspectives, followed by an interactive visit on the third day to India's nodal agencies dealing with cyber security; the Indian Computer Emergency Response Team and the National Critical Information Infrastructure Protection Centre. The participants at the workshop deliberated on various issues of importance concerning cyber security in the BIMSTEC context; the national perspectives and various aspects of

[2] "BIMSTEC Mechanism", at https://bimstec.org/?page_id=1761.

[3] "First meeting of the BIMSTEC National Security Chiefs (March 21, 2017)", Ministry of External Affairs, at https://mea.gov.in/press-releases.htm?dtl/28193/First_meeting_of_the_BIMSTEC_National_Security_Chiefs_March_21_2017.

international developments related to cyber norms and cyber crime; cyber security for digital economy; cyber incident response; and the protection of critical information infrastructure. The participants also adopted a Roadmap for BIMSTEC Cyber Security Cooperation.

* The workshop was a combined effort of Institute for Defence Studies and Analyses, National Security Council Secretariat, Ministry of Electronics and Information Technology, Indian Computer Emergency Response Team (CERT-In), Ministry of External Affairs, Ministry of Home Affairs, National Critical Information Infrastructure Protection Centre and the BIMSTEC Secretariat. The role of rapporteurs, Mr. Jyotishman Bhagwati, Ms. Sanya Saroha and Ms. Nivedita Kapoor in penning down the proceedings of the workshop is highly appreciated and duly acknowledged.

Session I: Inaugural Session

Introductory Address by Mr. Pankaj Hazarika, Director (CS), BIMSTEC Secretariat, Dhaka.

When the BIMSTEC was established in 1997, the Leaders of the Member States advocated for peaceful and progressive development in the region. Subsequently the Leaders have identified the fight against terrorism and transnational organized crime as one of the important prerequisite for sustainable growth and maintenance of peace in the region.

The First BIMSTEC Summit held on 31 July 2004, at Bangkok, Thailand expressed grave concern at the continuing threat of international terrorism and transnational crime that has adversely affected the economic and social progress of the peoples of the BIMSTEC region and recognized that the solidarity and friendship existing among member states could be utilized as a basis to counter this threat. The Leaders agreed, as an urgent priority, to coordinate efforts to combat this menace; including through the exchange of information among concerned agencies, and other concrete programmes of co-operation, and resolve to continue active co-operation in ongoing efforts of the international community in combating terrorism in all its forms and manifestations, by whosoever it is perpetrated irrespective of its cause or stated rationale.

Taking note of the emphasis placed by the First Summit on combating terrorism and transnational crimes, the 8th Ministerial Meeting held at Dhaka, Bangladesh on 18-19 December 2005 added Counter Terrorism and Transnational Crime (CTTC) as one of the priority sectors of BIMSTEC. India is the Lead Country of this Sector. The sector conducts its business through the Joint Working Group on Counter Terrorism and Transnational Crimes (CTTC). The First Joint Working Group Meeting on Counter Terrorism and Transnational Crime (JWG-CTTC) held in New Delhi in December 2004 had decided to establish four Sub-Groups on intelligence sharing, financing of terrorism, legal and law enforcement issues and prevention

of trafficking in narcotics and psychotropic substances and also decided to entrust the task to four Lead Shepherds- Sri Lanka, Thailand, India and Myanmar respectively. With addition of Sub-Group on Human Trafficking and Illegal Migration and Sub-Group on Cooperation on Countering Radicalization and Terrorism in 2017 the total number of Sub-Groups now stands at six.

BIMSTEC Leaders at their Retreat held in Goa, India on 16 October 2016, had recognised that terrorism continues to remain the single most significant threat to peace and stability in the Bay of Bengal region. The Leaders agreed to convene Annual Meeting of National Security Chiefs of Member States on Information and Intelligence Sharing.

The Government of India hosted the First Meeting of the BIMSTEC National Security Chiefs in New Delhi, India on 21 March 2017. The Meeting noted that BIMSTEC Member States face common security challenges and underlined the necessity of addressing these security challenges to harness economic prosperity and human security in the region in a sustainable and pragmatic manner. The Meeting underscored the importance of recognizing the Bay of Bengal as common security space.

The Meeting emphasized the necessity of deepening mutual cooperation among the Member States and noted that the BIMSTEC Member States are particularly vulnerable to threats from terrorism, violent and extremist ideologies, narcotic drugs, arms and human trafficking, threats in cyber space, maritime space, natural disasters, sea level rise due to climate change and other non-traditional security challenges. The Meeting noted with concern the emerging trends in cyber space which encourage online radicalisation, cybercrime and threat to the critical information sectors of the economy. The Meeting decided to deepen cooperation among the respective cyber institutions to strengthen cyber security. The Meeting agreed to a Joint Forum to strengthen cyber security among the BIMSTEC Member States. The Meeting decided to establish a Track 1.5 BIMSTEC Security Dialogue Forum to promote and encourage security dialogue among BIMSTEC strategic community.

The 2nd Meeting of the BIMSTEC National Security (NSA) was held in Dhaka on 28 March 2018. The threat from the cyber space was widely deliberated in the meeting. National Security Adviser to Hon'ble Prime Minister of India spoke about creating a BIMSTEC vision on sharing experience and pooling in resources to deal with cyber security and various other problems and threats. He

also recommended creating common platform for research in this area and to enhance capacity building in security related sectors.

National Security Advisor of Sri Lanka in his speech stated that cybercrime requires new approaches in combating terrorism. He also stated that cyber security could be achieved through multilateral cooperation and intelligence sharing among the member states. Deputy Secretary General, Office of the National Security Council, Thailand stated that most countries lack capabilities to protect their cyberspace from borderless and trans-boundary threats. India proposed in the meeting to organise a three day workshop of technical experts in the areas of IT and cyber security to discuss evolving cyber threat scenario in the region and explore cooperation at the working level to address cyber security issues of the Member countries in the BIMSTEC region.

This cyber security workshop of the BIMSTEC Member States is being held with this background the Leaders of the BIMSTEC Member States in the Fourth BIMSTEC Summit held at Kathmandu, Nepal on 30-31 August 2018 reiterated strong commitment to combat terrorism and call upon all countries to devise a comprehensive approach in this regard which should include preventing financing of terrorists and terrorist actions from territories under their control, blocking recruitment and cross-border movement of terrorists, Countering radicalization, countering misuse of internet for purposes of terrorism and dismantling terrorist safe havens.

Out of the six BIMSTEC CTTC Sub Groups, which I have stated earlier, the Sub Group on Anti Money Laundering and Combating the Financing of Terrorism has been deliberating on the issues of cyber security in its meetings. At the Ninth Meeting of the Sub Group held in Yangon Myanmar in April 2017, one of the Agenda was presentation of case studies by the Member States on the Emerging Cyber Threats on Financial Sector.

The issues of Cyber security were extensively deliberated by the First BIMSTEC 1.5 security Dialogue Forum held in this same venue on 21 September 2017. With the increasing technological up gradation and expansion, the world is witnessing a surge in cyber security threats that can affect individuals, organizations as well as the states. The case of Cyber Robbery that happened in Bangladesh in February 2016 where the hackers made fake transactions to Bangladesh Bank through a Bank in New York wherein certain amount was diverted to Sri Lanka and Philippines was an important case of cyber war which makes a compelling

case for greater cooperation to meet such challenges in the future. Another related issue in this context is sharing of data with other stakeholders and countries and the extent of data sharing. The Forum made these recommendations:

- *Set up a joint BIMSTEC countries' forum for deepening cooperation in the area of Cyber security and regular meetings of this forum should be held to tackle all the emerging issues. CERT (Computer Emergency Response Team) to CERT cooperation Forum may be set up with holding of regular meetings.*
- *Create a Task Force that would do diagnostic study and prepare country reports (on each country's capacity and vulnerability) on cyber threats. Capabilities of each Country are to be mapped. 5*
- *Partnering with each other to enable innovation and growth in digitization; strengthening investment cooperation in cyber area; and encouraging partnership among industries/organizations for capacity enhancement of SMEs in cyber-security.*
- *Government, Think Tanks may be encouraged to take initiative to create citizen awareness on cyber security & legal frameworks for cooperation may be decided.*
- *increase cooperation between citizens of the BIMSTEC countries which would bring together professionals of different countries and would also help common people of all the countries in the grouping and enhance law enforcement cooperation to address cyber-crimes.*
- *More focus may be given on capacity building and skill development. Member States may work together to formulate common position on cyber security issues at various international forums.*

Joint Working Group on CTTC held at Dhaka, Bangladesh on 13-14 August 2018 agreed that the Secretariat will segregate the recommendations of the Track 1.5 security Dialogue Forum subject wise and will include the recommendations in the agenda for deliberations by the CTTC Sub-Groups and various Expert Groups that have been constituted to deal with various non-traditional security issues. As the first measure the Secretariat has proposed the recommendations pertaining to countering radicalization as one of the Agenda of the upcoming Sub Group Meeting on Countering radicalization and violent extremism. However, as there is no formal mechanism e.g. working group, expert group established to deal with cyber security issues, the recommendations haven't been further discussed.

Combating international terrorism, transnational organised crime and illicit drug trafficking remain the core of security cooperation among the BIMSTEC Member States. BIMSTEC Convention on Cooperation in Combating International Terrorism, Transnational Organized Crime and Illicit Drug Trafficking was signed in 2009. So far six Member States have ratified the Convention. Once ratified by the remaining Member State, which we are expecting soon, this convention will be the basis for future cooperation in the CTTC Sector. Cooperation in the three specified areas i.e. international terrorism, transnational organised crime and illicit drug trafficking will now naturally involve cooperation in cyber security due to use of IT platforms, tools and social media in propagating these crimes. Further, the Convention also provides for cooperation in any matter as mutually agreed upon between the State Parties.

With increasing focus on digital connectivity, which has become a necessity to promote other forms of connectivity including trade and transport connectivity, cyber security has become and will continue to be the vital area necessitating cooperation among the BIMSTEC Member States. We hope that the deliberations in this conference amongst the experts on the subject will bring out concrete and pragmatic suggestions which can be recommended to the Member States for consideration.

Inaugural Address by Sh. Rajinder Khanna, Deputy National Security Advisor, Government of India.

The Bay of Bengal Initiative for Multi-Sectoral Technical and Economic Cooperation (BIMSTEC) is the international organisation of seven nations of South Asia and South East Asia, which is working towards a safe and secure regional security environment. BIMSTEC Community is charting a new path forward in new areas such as cyber security by coming together to address emerging security challenges emanating from cyberspace, underpinned by technological innovations and blurring of national boundaries in the cyber domain.

We are at the cusp of a very exciting time, with tremendous opportunities. The internet is now the backbone of our banks, power grids, business and governments. The inter-connectedness of internet, underpinned by ICT technologies and the ability to move data across borders, provides new avenues for economic development and growth.

Digital data is being called the new "oil" as it is an increasingly revenue source for many technology companies. Innovation is increasingly based on digital technologies and business models that effectively utilise opportunities offered by cyber domain. Technological advances on the horizon, such as artificial intelligence, IoT and robotics, are expected to change the way we live and work. Countries that are prepared and digitally engaged will be better placed to ride this revolution.

Yet while this digital revolution has spurred new opportunities, it has also spawned new threats. These cyber threats continue to grow in scale, sophistication and severity from hostile states, groups and individuals who use cyber medium and tools to commit cybercrimes and cyber terrorism, to project power, to intimidate their adversaries, and to influence and manipulate societies and citizens.

We have moved into an era of increasingly complex cyber threats. Our growing digital dependence means that vulnerabilities can have widespread, unpredictable, and cascading consequences. For instance, in 2017, more than 300,000 computers in 150 countries were hit by the Wannacry ransomware attack, with cases reported in BIMSTEC countries including India, among others. And then of course, there's the broader cyber threat to national, regional and international security. Hostile state activity in cyberspace is the most alarming expression of that threat. Many states are building cyber capability. This has led to "trust -deficit" among states and thus has potential to disrupt regional and international security environment.

Cyber security also raises important issues for personal privacy and the data protection. Advancement in technology such as Data Mining, Big Data Analytics, Cloud computing etc. brings unforeseen challenges and one of the major challenges is threat to "privacy" and Data Protection. The Facebook–Cambridge Analytica data scandal (2018) revealed that Cambridge Analytica had harvested the personal data of millions of people's Facebook profiles without their consent and used it for political purposes. All these have led to demand for data protection regime and data localisation. EU has implemented adopted General Data Protection Regulations (GDPR) from 25 May 2018. Similarly, many countries are working towards adopting data protection laws and data localisation. Cyber security is a common concern among states including BIMSTEC countries. BIMSTEC needs to address cybersecurity challenges to reap the full dividends of future digital economy.

Given the tremendous potential for digitalisation in BIMSTEC, there is great opportunity for BIMSTEC countries to play a leading role in area of cyber security to ensure region's future growth and development. As such, it is important that BIMSTEC countries work together collectively as a community to ensure a secure and resilient cyberspace in the region. The e-commerce space and the digital economy space are the new areas where cooperation within BIMSTEC can lead to prosperity and growth in the region.

India has embarked on the digital India programme to bridge the digital divide in the country and access to internet. Today, India has the world's second largest numbers of internet users after China. Aadhaar is world's largest biometric database of more than a billion Indians. India's digital economy is growing with emphasis on digital payments/ online financial transaction. The Government has

taken a number of steps to ensure a safe and secure Indian cyberspace and strengthen the cyber resilience of the critical information infrastructures (CIIs). Major cyber security initiatives includes the 2013 National Cyber Security Policy, Information Technology Act 2000, setting up of CERT-In and NCIIPC as nodal cyber agencies under IT Act, Draft Personal Data Protection Bill 2018, measures to strengthen privacy and data protection, promotion of cyber security R&D, capacity building and skill development, promotion of public-private partnership in cyber security. But for all that we've done, and for all that we're doing, there's still much more work ahead. And what bring us all here today is the recognition that we cannot do it alone. We should continue stepping up similar efforts within each of our countries, so that we can collectively create a safer and trusted cyberspace, and combat cyber threats with better capabilities.

We need to work together within and beyond BIMSTEC to minimize cyber risks by raising the level of regional capacity and cooperation in the area of cybersecurity. This workshop is aimed at initiating regional capability building in all aspects of cyber security and to heighten the awareness of ongoing global cyber norms discussions at international platforms such as the United Nations Group of Governmental Experts (UNGGE).

India is committed to foster close relationships with our BIMSTEC counterparts to build up regional cyber capacity, and will be deepening our support to this end. Besides scaling up cyber capabilities, we can collectively develop and agree upon basic voluntary cyber norms in BIMSTEC region. This will be useful to amplify BIMSTEC's voice on international cyber discussions at international forums such as the United Nations, UNGGE.

India is supportive of having basic rules for responsible state behaviour in cyberspace and believes that BIMSTEC can work together to reach consensus on basic voluntary cyber norms for the region. I would like to put forth a call for greater coordination among BIMSTEC on cyber policy and capacity building so that we can project a unified BIMSTEC voice internationally to protect and advance our regional perspectives.

We should work towards further strengthening partnerships with similar regional and international organizations such as the United Nations, BRICS, SCO, EU, OSCE, ARF, to identify and respond to trans-boundary threats in a timely, coordinated and coherent manner. A coherent, coordinated global effort is key to a trusted and resilient cyber environment. There is a need for sharing of

information among states and working together to effectively respond to trans-boundary cyber threats.

Cyber technologies are evolving continuously, from the Internet of Things (IoT) to 5G to artificial intelligence to quantum computing, and each advance is accompanied not only by new opportunities, but new challenges. Cyber security is a shared responsibility. We need to work together to strengthen cyber security to take full advantage of this technological domain. Present Cyber Workshop provides us opportunity to deliberate on common cyber security concerns, share experiences and create a roadmap to move forward as a united and cyber-resilient region. I look forward to the meaningful discussions in the workshop, and wish all of you a fruitful time in New Delhi.

Session II: Cyber Security Preparedness and National Approaches of the BIMSTEC countries to secure cyberspace

Chair: Dr. Ajeet Bajpai, Director General, National Critical Information Infrastructure Protection Centre (NCIIPC).
Co-Chair: Dr. Ajey Lele, Senior Fellow, IDSA.

Dr. Ajeet Bajpai opened the session by underscoring the fact that internet is intertwined with our modern lives and one cannot deny the vulnerabilities that individuals are exposed to. These threats are more disruptive and are moving towards being destructive. Moreover, the transnational characteristics of the threats makes the issue much more complex. He categorized these threats into four categories:

- The first one is *known*, and it can be mitigated as they are well documented and the mitigation strategies ensure that cyber security system is well in place.
- The second one is where the threat is *known but the mitigation is not immediately available,* and it is due to various reasons like lack of legal framework or technological shortcomings.
- The third category belongs to those threats which *exists but one doesn't know about them*. These are also known as zero day vulnerabilities, and in such cases, the only option is to have a multi-stakeholder approach to deal with it by keeping one's eyes and ears on the ground and at the same time cooperating and coordinating with various agencies in the system.
- The last but not the least, are those threats which are *evolving* and this is the most dangerous of all the categories. A defender's job in this case is the toughest, since he has to defend successfully numerous threats all the

time, but attacker has to succeed only once. With these remarks he opened the session for the speakers.

- ***Bangladesh perspective*** **by Md. Sakhawat Hossain, Superintendent of Police (SP), Special Branch, Bangladesh Police, Bangladesh.**

  Md. Sakhawat Hossain reiterated the dependence of people on the Internet in the 21st century, which encapsulates the domains like financial services, commerce, transportation, medical facilities etc. Highlighting the rising menace of cyber crime as a transnational crime, he brought out the Bangladesh perspective as it intends to develop as a digital economy and a middle-income country by 2021. Keeping in view the aspirations of the country and the challenges to its digital economy, Bangladesh has already established a Cyber Emergency Response Team (CERT) and also established a cyber-tribunal and cyber appellate tribunal under its National Cyber Policy of 2006. On the legal front, Bangladesh has enacted four legislations: Pornographic Control Act, Information and Technology Act, ICT Act, and Digital Security Act. The main problem in Bangladesh, as per Md. Sakhawat Hossain, emerges from the social networking sites which are used to execute criminal acts and incite communal riots. He further stressed on the need for global partnerships to address these outstanding issues in cyberspace.

- ***Bhutan Perspective on Cybersecurity Initiatives, Challenges and Issues*** **by Ms. Sonam Choki, Sr. ICT Officer, Bhutan CIRT.**

  Ms. Sonam Choki gave a brief overview of the evolving cyber security practices in Bhutan, as she noted that Internet has penetrated into all domains of the Bhutanese society ever since Bhutan connected to the Internet in late 1990s. Bhutan has various policies in place to deal with cybersecurity activities, with the Bhutan Information and Communications and Media Act (BICM Act) being enacted in 2018. In 2009, Bhutan had come out with an Information Management and Security Policy. Bhutan is also working on a Cyber security Strategy, which is in the draft stage presently. Ms. Sonam Choki elaborated on the Bhutan Social Media Policy which established a code of conduct for the Bhutanese civil servants.

  Bhutan is also developing its cyber security education policy to spread awareness and train professionals in the subject. The Bhutan CIRT (BtCIRT)

started operations in April 2016 and its mandate is to serve as a central coordination point of contact at the national level. Bhutan has also conducted cyber simulation exercises for Ministers, CEOs and heads of critical sectors and organizations. It also conducts continuous IT trainings and educational initiatives with Public and Private sectors. However, the main challenge for Bhutan, as per Ms. Sonam Choki, is the lack of funds, technical skills and knowledge of ICT as well as the lack of awareness among citizens and Bhutan still lacks a framework for protecting children online.

- ***India perspective*** **by Dr. Sanjay Bahl, Director General, CERT-In.**

  Dr. Sanjay Bahl presented the India perspective and he opened his remarks by stating that a country needs to have a holistic approach to deal with cyber security. The critical infrastructure needs to be protected from any threats emerging from the cyber domain. India's digital profile and footprint is one of the fastest growing in the world, and the flagship programs like Jan Dhan Yojna, Aadhaar, and growing mobile networks are part of India's digital evolution. At its current pace, India's digital economy is estimated to reach USD 1 trillion by 2025. Dr. Bahl warned that any form of breach may have a huge impact on the country's security matrix. He further elaborated on the following cyber security approaches:

  - National Level Policies
  - Regulatory and Legal frameworks
  - Cyber Security Incident Management
  - Assessment and Assurance
  - Critical Infrastructure Protection
  - Capacity Building

  He explained that India has taken strong steps to protect its digital economy. The National Cyber Security Policy of 2013 clearly articulates the prevailing concerns, and it is pivotal in understanding priorities for action as well as for directed effort. The Framework for Enhancing Cyber Security was set up to respond to any incident related to cyber crime or cyber attack. The vision is to build a secure and resilient cyberspace for the citizens on India. The implementation of India's cyber policy, as explained by Dr. Bahl, is through three layers: government, public-private cooperation and private organizations. India has also enacted some national cyber policies and legislations. The

government is also working towards updating its national cyber security structures for sound implementation of policies and legislations by clearly defining roles and actions of each player and institutions. India is also making efforts towards building a financial CERT and other sectoral CERTs. In a more holistic manner, as per Dr. Sanjay Bahl, building cyber resilient systems will have a force multiplier effect in enhancing cyber security.

- ***Myanmar Perspective*** **by Mr. Soe Naing Oo, Police Brigadier General, Criminal Investigation Department, Myanmar.**

  Presenting the Myanmar perspective, Mr. Soe Naing Oo pointed out the national cyber security measures Myanmar has adopted in recent times, taking into consideration the rising number of users of mobile phones and social media platforms. In 2011, Myanmar government had established a cyber Security Steering Committee and it has also undertaken an initiative to set up a National Cyber Security Center. Mr. Soe Naing Oo categorized cyber crimes which range from fake websites, online gambling and fraud to child pornography, and highlighted that a bill is under progress to address this issue. Mr. Soe Naing Oo stressed that the cases of cyber crime have decreased in 2018 as compared to 2017 due to proactive policies. On the aspects of Public-Private cooperation, he highlighted the examples of Myanmar Computer Science Development Council, Myanmar Computer Federation and the Ministry of Transport and Communications, which are all playing a positive role in cyber security for the government and citizens of Myanmar. Major challenges faced by Myanmar, as per Mr. Soe Naing Oo, are the lack of awareness of cyber threats and lack of skilled professionals in this domain. He said, going forward, there has to be a regional approach to deal with cyber crime through cooperation and close engagement with the international community.

- ***Cyber Security in Nepal*** **by Mr. Rabin Basnyat, Chief of Digital Forensics, CID, Nepal Police.**

  Nepal's internet penetration is one of the fastest among the BIMSTEC Member States. Speaking on Cyber Security in Nepal, Mr. Rabin Basnyat noted that there was no national cyber security policy or strategy in Nepal before 2015. Owing to the gravity of the cyber threats, there was a dire need to address the root causes

of cyber threats. In 2015, a cyber security awareness assessment by the National Telecommunications Authority led to the creation of National Cyber Security Awareness Program. Major cyber crime initiatives, including setting up of a Digital Forensics Lab in May 2016, were part of the outcome of the assessment. Additionally, specialized investigative units were also set up to deal with cyber crime.

A draft cyber security policy was prepared in September 2016 and an IT Act also being charted out. Mr. Rabin Basnyat further delved into social media related cyber crimes, website hacking, data theft, unauthorized access and financial frauds in internet banking as some of the major cybercrime trends observed in Nepal. According to him, Nepal is in constant interaction with the international community, such as Interpol and stakeholders of financial sector to improve security. Outlining the way forward, he explicitly mentioned that it has to be a top down approach and not a bottom up one, and intermediary solutions need to be worked upon and capacity building needs to be prioritized for BIMSTEC countries to succeed in this endeavour.

- ***Cyber Security Readiness in Sri Lanka & Way Forward*** **by Mr. Rohana Chaminda Akmeemana Palliyaguru, Director-Operations, Sri Lanka CERT|CC, Colombo.**

Bringing in a national security perspective to cyber security, Mr Rohana Palliyaguru reiterated that dealing with cyber crimes requires a top-down approach and it is deeply connected to national security. Although Sri Lanka's internet usage is very low, mobile penetration is over 100 percent, and similar to other Member States, cyber crime incidents in Sri Lanka are on the rise. Most of the cases reported in Sri Lanka, according to Mr. Rohana Palliyaguru pertain to social media, while pornography, copyright violations and misuse of phone numbers are also prevalent. The evolution of cyber security in Sri Lanka began with the e-Sri Lanka initiative by the Information and Communication Technology Agency in 2005, leading to various online initiatives.

He further elaborated the role of Sri Lanka CERT, which was established in 2006 to provide technical advice and assistance to the Sri Lankan government, and it is now a full member of Asia-Pacific CERT and FIRST. Sri Lanka has also established a cyber crime division at CID to prosecute cyber security incidents and the Computer Crimes Act No. 24 of 2007 provides the legal framework for a broad range of offences. Sri Lanka is also a part of the Budapest

Convention, becoming the first country in South Asia and the second country in Asia after Japan to accede to the convention. He informed that Sri Lanka is also on its way to develop a National Cyber Security Strategy under a five year programme (2019-2023), and the key areas for the strategy are:

- Prioritizing Cyber Security Issues;
- Securing Government Systems (As unprotected systems may actually hamper the citizens trust on governmental agencies);
- Creation of legal and institutional framework; and
- Competent Work Force.

- ***Thailand Perspective*** **by Ms. Rawinnipa Karin, Plan and Policy Analyst, Directorate of Countering, Transnational Threats, Office of the National Security Council (NSC), Thailand.**

  Presenting the Thailand perspective, Ms. Rawinnipa Karin reiterated the implications for national security from cyber threats. Thailand envisages a secure and safe cyberspace and all the sectors should be well-prepared to handle cyber incidents as part of the national security preparedness. The cybersecurity readiness assessment, according to Ms. Rawinnipa Karin, was prepared considering the new and emerging trends of cyber threats to the government, private sector and the citizens. Such measures are vital for the economic stability of Thailand and the quality of life of its citizens. She also touched upon the National Cybersecurity Strategy 2017-2021, which encompasses protection of critical information infrastructure, preservation of national interest in cyberspace, cooperation with other countries and boosting overall growth of Thailand. The most urgent tasks before the Government are developing human resources specializing in cyber security, strengthening the defences of Critical Information Infrastructure Protection, raising awareness and enacting the Cybersecurity Act which is still in a drafting stage.

- **Co-Chair: Dr. Ajey Lele.**

  Summarizing the session on BIMSTEC perspective, Dr. Ajey Lele stressed that it is pertinent to understand the respective approaches of BIMSTEC member states to tackle threats and chart out the way forward. Also, understanding the strengths and weaknesses of each country *vis-à-vis* cyberspace is important, as

collaboration needs a certain level of clarity of roles, rules and regulations prevalent in the respective Member States.

He noted that Member States have to understand each other's needs and constraints first, in order to make cooperation viable in the case of BIMSTEC. Moreover, cyber threats, according to him, should not only be bracketed under cyber crime, but it should rather be looked at from a broader landscape of cyber warfare as well. Summarizing the outcomes of the session, he discerned that immediate challenges in capacity building have been sharing of experiences, raising awareness and training, and going forward a top down approach may be considered to address the issue.

Session III: Regional Challenges in Cyber Security and Cyber Crime in BIMSTEC countries

Chair: Dr. M. M. Oberoi, ICT Advisor, MHA.
Co-Chair: Mr. G. Narendra Nath, Deputy Director General (Security), DoT.

Dr. M. M. Oberoi gave a brief introduction to the challenges of law enforcement, forensic capabilities as well as the multi-jurisdictional issues that affect cyber security. Capacity for law enforcement agencies, in terms of manpower, skill-set, analysis, investigation etc. is the prime issue. With these brief remarks, he opened the session for speakers.

- **Mr. Sreejesh, Ministry of Home Affairs.**

  Speaking of the expanding threat landscape and increased sophistication and capability of cyber attacks, Mr. Sreejesh classified threats and vulnerabilities as both internal and external. He highlighted the broad trends such as the targeting of sensitive sectors, growing sophistication of malwares, meticulous planning of the cyber attacks and the use of compromised systems to launch attack against other countries. The growing number of web based applications and digitization of services has increased the vulnerabilities in government infrastructure. He delved into the various factors which impinge cyber security, such as the lack of cyber hygiene and the dependence on outsourcing partners which even handle sensitive information. On the aspect of social media challenges, he noted the rising threat from unverified user accounts, anonymity on such platforms, vast volumes of data and multi-media generated and the veracity of content which is not checked for authenticity before going online. The way forward, as per Mr. Sreejesh, is that BIMSTEC Member States form cyber threat intelligence groups and cyber defense forces.

- ***Data Protection and Privacy*** **by Mr. Somnath Banerjee, Country Manager, Training & Enablement, McAfee.**

  Security threats have increased with the advent of mobile devices and smart phones, and Mr. Somnath Banerjee presented statistics related to this proliferation of smart phones and networked devices. It is estimated that by 2025, 75 billion smart connected devices will be in existence, which are well-known for leaking and extracting information. In such a world of connected smart devices, it would become difficult to protect one's personal data and information. Privacy permeates to all stages from data collection to data dispersion or storage, and therefore, cyber security has to be built-in to enable data protection at all the levels. He further touched upon Darknet, which is extensively used in criminal activities and concluded that strong cybersecurity and privacy protection is a journey, not a destination.

- ***BIMSTEC Cyber Threat Landscape*** **by Mr. Oleg Abdurashitov, Head of Public Affairs, Asia Pacific, Kaspersky Lab.**

  National development is not possible without economic progress, which further depends on digital technologies. These technologies create potential risks and

vulnerabilities to national security. Mr. Oleg Abdurashitov termed it as a vicious circle which cannot be ignored and presented data gathered by the Kaspersky Lab. As per the data, Bangladesh and India witness the highest number of mobile malware attacks among the BIMSTEC Member States and they are also amongst the five most attacked countries in the world. Based on the data, India faces the seventh most IoT attacks globally. He further delved into the Advanced Persistent Threats (APT), as the trends suggest that they are moving to brand new paradigms, with destructive malwares being used in geopolitical conflicts. There needs to be transparency, cooperation and mutual understanding among the respective organisations from the BIMSTEC Member States to tackle the rising menace of cyber threats.

- **Mr. Rajiv Singh, Tech Mahindra.**

  Presenting a broader overview on the present trends in cybersecurity, Mr. Rajiv Singh touched upon the aspect of economic cost of data breaches, behavioural analytics, advanced threat management, and cloud security. The speed of response to any cyber incident is important since the damage in the first few hours (also known as the golden period) is the maximum. On the point of advanced threat management, Mr. Rajiv Singh asserted that the complexities of cyber attacks cannot be defended through traditional means.

- **Brig. Ashish Chibbar, Senior Fellow, IDSA.**

  Brig. Ashish Chibbar presented few facts to underscore the urgent need to elevate cyber defences. Over 25 percent of global internet users reside in the BIMSTEC Member States. Although the mobile internet speed in the BIMSTEC Member Studies is the lowest, but it generates largest mobile traffic. He observed the growing e-commerce penetration in the BIMSTEC Member States which is a great opportunity for the future. He also noted a reduced role for the United Nations in the near future but a prominent one for bilateral and regional engagements and also a region-oriented norms building process. The Internet is increasingly becoming a part of the national security matrix and it is no longer a merely a source of entertainment or infotainment. A safe and secure cyberspace environment is essential for the further development of BIMSTEC Member States.

Brig. Ashish Chibbar asserted that data thefts will increase in the future and made few observations related to the increasing frequency of zero day exploits, financial frauds and crime, unauthorised harvesting of personal data, use of crypto currencies in cyber crime, and psychological and deception campaigns in and through cyberspace. According to him, the way forward is to make ICT companies accountable and shared partners in cyber security, invest in human resource, innovations and awareness.

- **Mr. Vivek Chudgar, Fire Eye.**

Mr. Vivek Chudgar spoke from the point of view of cyber risk management, stating that it requires managing threats and controlling vulnerabilities, however managing vulnerabilities is a traditional option but not a viable one since companies today do not operate within a single boundary. He underscored that 'one size fits all' approach is insufficient for cyber threats and enterprises need to build a security architecture taking into account its unique requirements, technology, attack surface and characteristics. He asserted that it is pertinent to have an integrated IT/OT incident response plan and specific monitoring and detection needs Industrial Control Systems (ICS) to be enhanced.

- **Mr. Aneesh Dhawan, Microsoft.**

Cyber threats have completely changed in their shape and form as well as in their complexity. Mr. Aneesh Dhawan touched upon the motivational factors for the attackers, which are growingly commercially now. An attacker today wants to remain anonymous, since it is not about fame anymore, but the data is the prime target now. He also informed that ransomware attacks and malware download rate are very high in BIMSTEC Member States. As recommendations, Mr. Aneesh Dhawan, underscored the relevance of better threat protection, enhanced identity protection (through machine learning and AI) and augmented data protection (through ensuring a zero trust network). A better solution, according to him, would be to reduce vendors and chose the one which provides more efficiency and makes security simpler for the enterprise.

Session IV: International Cyber Politics and Governance – Opportunities and Challenges

Chair: Mr. Upender Singh Rawat, JS (Cyber Diplomacy), Ministry of External Affairs.
Co-Chair: Mr. Soe Naing Oo, Police Brigadier General, Criminal Investigation Department, Myanmar.

Mr. Upender Singh Rawat articulated the various efforts being undertaken at the global stage to develop norms of responsible state behaviour in the realm of cyberspace. He noted the efforts made under UNGGE and Budapest Convention and highlighted the role of regional organisations in such processes. He added that further talks are needed on matters like complex technological changes and the transnational nature of cyber issues. On the topic of Budapest Convention, he noted that a similar framework does not exist under the aegis of the United Nations and India had concerns regarding some articles in the convention that it believed had implications on its national sovereignty.

- **Mr. Rahul Gosain, Director, Ministry of Electronics and Information Technology.**

  In the context of data protection, Mr. Rahul Gosain spoke about the General Data Protection Regulation (GDPR) which came into force this year. As a data protection law, it has the potential to change the way cyber security and intellectual property enforcement is carried out globally, although it is specific to the European Union. He also highlighted the increasing popularity of social media and the imminent threat from fake news which needs an immediate

response. Mr. Rahul Gosain argued for a heightened understanding of new technologies and to bridge the digital divide between the global south and north, in addition to promoting local language content on the Internet. He underscored the need to ensure that systems are built to ensure privacy as well as to study the impact of GDPR implementation beyond the EU borders as cyberspace is not just restricted to a single country or continent. He concluded by saying that cyber governance must be undertaken by keeping in mind the local realities and global competitiveness.

- **Mr. Munish Sharma, Consultant, IDSA.**

  Mr. Munish Sharma linked technology with economic development and highlighted that all the BIMSTEC Member States are developing countries and it is pertinent for them to understand the criticality of the cyberspace as it presents both the scope of growth and means of vulnerability. He categorised international politics into three dimensions namely – Technology, diplomacy and security. He pointed out that as developing countries there is a lack of infrastructure and skilled human resources, which in a way negatively impacts their ability to assert their voice and make rules at the global level where the leaders in the field dominate any discussions and policy decision thereof.

  He proposed setting up of a regional innovation hub and engagement between research intuitions or laboratories in the BIMSTEC Member States to enable innovators in converting their ideas into world-class products and services. He also noted the need for effective attribution of cyber attacks, especially in cases where critical infrastructure has been disrupted, arguing for the need to form investigative groups within BIMSTEC Member States which can aid cross border investigation and bring perpetrators to justice. He articulated that since BIMSTEC Member States have no unresolved bilateral issues, hence cooperation should not be a tough nut to crack. He concluded by recommending that the BIMSTEC members must add a development agenda to the formation of cyberspace norms as a group of developing countries with a unified voice.

- **Ms. Rehana Parvin, Assistant Secretary (BIMSTEC), Ministry of Foreign Affairs, Bangladesh.**

  Ms. Rehana Parvin raised concerns about the increasing malicious cyber activities and cyber attacks and pointed out that cyber security cannot be carried out in isolation. The major challenges of consensus building, lack of awareness, lack of political consciousness and lack of technological development were highlighted as main problems being faced by developing countries in dealing with cyber security. She also underscored the need for cooperation and collaboration among multiple stakeholders for policy making and development of legal frameworks.

- **Brig. Abhimanyu Ghosh.**

  Brig. Abhimanyu Ghosh shed light on the norms making process in cyberspace and stressed that state sovereignty should be honoured. He dwelt on the history of efforts to build norms for cyberspace, especially the role of UN Group of Governmental Experts (UNGGE), drawing from his personal experience of being involved in the process. He asserted that though the international law applies in cyberspace, the application of the same has been a source of deliberations among the international community. He highlighted the need for confidence building measures that enhance mutual trust in the digital world and prevent any escalation that might hinder global stability, especially militarisation of cyberspace. He also spoke of the need for developing countries to undertake capacity building where IT penetration is low to ensure all the countries are able to implement the norms.

  In the case of BIMSTEC, he said that the Member States can analyse the specific needs of each Member State and make a strategy besides looking at mechanisms for public private cooperation. He concluded by shedding light on the process of due diligence being a part of law, that is, a country should not only ensure that one's ICT is protected but also ensure that it is not used to target other nation's assets and systems. Though he realised that funding and finance to implement such measures would remain a challenge, but few steps can augment the process, such as identifying the stakeholders involved and their role in the cyber security matrix, CERT-to-CERT cooperation and bilateral arrangements, and respect the diverse cultural heritage of each of the Member States to form a unified voice for the region.

- **Co-Chair: Mr. Soe Naing Oo.**

  The co-chair, summing up the proceedings, dwelt on the difficulty in enforcement of traditional law and order practices to tackle cybercrimes as they increasingly have become complex in nature. He also noted the difficulties associated with the lack of resources and funding in enabling cyber security measures. He suggested that there is a need for cooperation between multilateral organisations like BIMSTEC and ASEAN to improve the cyber security readiness of their respective Member States and the interactions should be more frequent and candid.

Session V: Developing Cyber Security Capacity – Technical and Institutional Challenges

Chair: Mr. Rakesh Maheshwari, Scientist G and Group Coordinator, Ministry of Electronics and Information Technology, (MeitY), Government of India.
Co-Chair: Mr. Weranchai Prayoonpruk, Deputy Director, Office of Cybersecurity, ETDA, Thailand.

In his opening remarks for the session, Mr. Rakesh Maheshwari mentioned the pace of technological development, stating that India itself has more than 450 million internet connections, population of around 400 million having smart phones and 1200 million phones. India captures the top ranks on the usage of social media platform, which means there is a high usage of Internet technologies and therefore it is prominent that risks and threats have also increased. Internet is virtual, border-less and anonymous and therefore legal,

institutional or people capacities should be developed and maintained in the country and in the region.

- **Co-Chair: Mr. Weranchai Prayoonpruk.**

  Taking forward the Chairperson's remarks, Mr. Weranchai Prayoonpruk said capacity building has been a major challenge among the BIMSTEC Member States, and simultaneously the rapid change in the technology space is leading to increase in cyber threats and the demand for cyber security professionals. Cyber security is all about people, processes and technology, however, many security initiatives have focused on the technology aspect alone. Capacity building is one of the important factors in shaping the cyber security practices, given the important role people play in building strong defences for the cyber assets.

- **Mr. Amit Sharma, Additional Director, Defence Research & Development Organisation (DRDO).**

  Mr. Amit Sharma started by highlighting that the contemporary cyber challenges need a paradigm shift in the traditional approaches to capacity building. In the last few decades digitalisation across South and South-East Asia has led to colossal changes. The threats landscape has also completely altered and it is affecting most of the ways in which one leverages cyberspace. The very advent of cyber terrorism, cyber crime and cyber warfare, according to Mr. Amit Sharma, underscore the changing technological and political milieu.

  He also brought in a historical account of the evolution of cyber weapons, and explained how they are akin to a missile system, which consists of a payload, a navigation system and a delivery vehicle. Delivery vehicles may be a website carrying a malicious links or could also include hacking, an email, or counterfeit hardware or software etc. Payload could be a program that copies information of the target and sends it to an external source or could just destroy the data. A very prominent example is the STUXNET attack, where the malware was later modified for DUQU and FLAME attacks, altering the payload.

  Mr. Amit Sharma further spoke about the need to build capacity according to the security matrix, given the new challenges like interdependent, intertwined and interconnected systems like nuclear reactors, dams, power grid. He also

touched upon the immediate need for new means and mechanisms for capacity building and law enforcement, to tackle the new-age issues like information enabled terrorism and the use of dark web and cryptocurrencies for illegal activities such as drug trafficking, arms trafficking, fake passports etc. He also emphasised on the need to revisit the security policy, regulatory compliance, user awareness programs, access controls, etc. and establish high level of partnership among regional organisations or economic groupings.

- ***New Challenges of Digital Forensics*** **by Ms. R. Ananthalakshmi Ammal, Centre for Development of Advanced Computing, Trivandrum.**

  Forensic challenges are the other side of the coin in cyber security, as they help in examining and analyzing the available digital evidence as part of investigations and assessments. Ms. R. Ananthalakshmi Ammal presented the challenges before digital forensics such as resources constraints, legal and technical challenges which include diversity of devices, volumes of evidence, use of encryption and anti-forensic techniques, steganography and cloud storage.

  She also underscored the implications for forensics from technology changes such as solid state drives, software defined storage, hard drive encryption for mobile phones, software defined networks, network visualisation and Darkweb. Ms. R. Ananthalakshmi Ammal proposed setting up of cyber forensics training programs and cyber crime analysis laboratories for better understanding of emerging technologies.

- **Dr. Cherian Samuel, Research Fellow, IDSA.**

  Dr. Cherian Samuel, speaking of confidence building and capacity building, stated that invariably it is the confidence building aspect that gets much higher weightage than capacity building, as security issues dominate the cyber realm. Confidence building, dating back to the Cold War era, continues to be seen as means of curbing conflicts whereas capacity building has been a part of the development paradigm. The process of capacity building needs to take into consideration the Government led processes, education, training and awareness programs, formulating of laws, R&D and innovation.

  All these broader themes should be linked to Capacity Maturity Model and a maturity assessment exercise can help in benchmarking existing capacities,

allow policy makers to access important information, and conduct simulation exercises. He concluded that all these if undertaken at a regional level may feed into the global conversation for cyber security and both confidence building and capacity building have to go hand in hand for a holistic cyber security approach.

- **Mr. Nitin Rai, DRDO.**

  Emphasising on the need to differentiate between cyber security capacity and cyber capacity, Mr. Nitin Rai explained that Cyber Capacity Building involves technological gaps and functional capacity building while Cyber Security Capacity Building includes understanding the emerging threats, known as well as unknown vulnerabilities, zero day attacks, and the role and capabilities of state and non-state actors.

  Major challenges have been understanding the rapid technological advances like cloud based storage, Blockchain technology, IoT, Quantum Computing. He noted that as attacks are evolving and malware is becoming increasingly complex, the way forward should include setting up of indigenous cyber R&D centres, assessment of assurance and trust factors, adequate training and awareness, and international cooperation. According to Mr. Nitin Rai, in order to enhance cyber security capacity, vulnerability assessment, compliance, audit of control measures, penetration testing, training and strengthened coordination and cooperation would be extremely important.

Session VI : Panel Discussion on BIMSTEC Cooperation in the Area of Cyber Security

Chair: Ms. Prabha Rao.
Co-Chair: Dr. Sanjay Bahl, Director General, CERT-In.

Initiating the panel discussion, Ms. Prabha Rao brought to light the existing aspects of crimes, hate crime, fake news, child pornography and fake videos. She insisted that BIMSTEC Member States should stand together and come up with provisions to maintain a database of people accused with charges of illegal activities and share the same across the region, as one of the means to tackle cyber crime.

- **Dr. S K Pal, Director (IT & CS), DRDO.**

  Cyberspace is now considered to be the fifth domain of warfare. This domain is utmost important as it provides interconnectivity and communications between the other four domains that is, air, land, sea and space. Dr. S K Pal, taking cue from these observations, noted that an enemy does not need an extensive ground troops or nuclear weapons to wage war anymore, all that is needed is inexpensive tools, some skills and access to a network, where the cost of entry is non-existent. Several actors working on the behalf of nation states or terrorist organizations seek access to information pertaining to copy rights, critical infrastructure and national secrets.

  A major challenge is that entire structures of software and hardware are not indigenously designed, developed and infrastructure may not be within the country itself. This gives rise to the danger of supply chain contamination. Citing the example of an incident where testers found a tiny microchip that wasn't a part of original design and these chips allowed the attackers to create a stealth backdoor. He emphasised that products like routers, switches, etc. are vulnerable, and recommended close collaboration among BIMSTEC Member States, establishment of facilities to test the COTS Products (routers, switches, etc.), development of encryption products and capability for malware reverse engineering.

- **Mr. Narendra Nath, DDG Security, DoT.**

  Drawing from his experience with the telecom sector, Mr. Narendra Nath said that one of the foremost challenges in the telecom sector is of incident response and legal framework. This sector is technology driven and telecom service

providers have a lot of technical expertise. Initially when the transactions were made, they involved voice communications and security was never an issue because of trust and assurance, but now the variety of digital devices and the number of end users has increased to such a level that security has to be built at every stage. On the issue of policy advancement in telecom sector, he mentioned that there is a checklist for policy implementation security audit. It is extremely challenging to have consistent processes across the country. He also informed that over the last two years, around 8200 people across the country have joined the telecom sector and they have also gone through intensive training programme on security, in addition to the operational knowledge of networks, 3G networks, mobile and landline networks. He pointed out the importance of having respective points of contact among BIMSTEC Member States, and identifying common issues to work together.

- **Mr. Pankaj Phukan, US (Cyber Diplomacy), MEA.**

  Mr. Pankaj Phukan noted that it is the first time that BIMSTEC Member States are discussing cyber issues, though there are a number of regional and multilateral platforms for it. To begin with, he said, it is important to highlight the priority areas like technical cooperation among BIMSTEC Member States and information sharing. In this context, regional cooperation is extremely important especially in the light of the growing race for building cyber norms. On international forums like the UN, BIMSTEC should emerge as a one voice, showcasing some form of regional consensus. There should be trans-border communication and maintenance of common standards for all. He emphasised that it is crucial to focus on building capacity and confidence in cyberspace and the way forward is to designate points of contacts to have regular interactions with experts as issues are technical and complicated at the same time.

- **Col. Sachin Burman, Deputy Director General, NCIIPC.**

  Mr. Sachin Burman informed that the National Critical Information Infrastructure Protection Center (NCIIPC) is mandated as a special body to cater for the protection of critical infrastructure in India. He drew attention to the previous discussions that the existing systems were not designed and build with security in mind and the environment therefore enshrines insecurity. He explained that along with the traditional cyber security, the NCIIPC is also

looking at the OT (operational Technology) aspects of smart grids and banking and financial services sector. Mr. Sachin Burman also touched upon the novel approaches to handle cyber issues such as responsible vulnerability disclosure programme which lets researchers to report vulnerabilities. There is also a need to differentiate between IT and OT aspects of cyber security to pave the way for holistic approach for tackling cyber threats.

- **Mr. Anoop Yadav, Dy. Legal Advisor, IS-II, MHA.**

  Speaking from legal and law enforcement point of view, Mr. Anoop Yadav noted that there are provisions in Mutual Legal Assistance Treaty where the state agencies can aid in prevention and suppression of malicious act, however, it entirely depends on the intent of the country to provide assistance to such requests. There are various aspects of information sharing, police to police cooperation as far as cyber security is concerned. The most important part, according to him, is preservation of time-critical evidence. He acknowledged that BIMSTEC Member States need to develop a mechanism to provide information at the earliest to assist each other in investigations and law enforcement.

- **Co-Chair: Dr. Sanjay Bahl.**

  Summarizing the panel discussion, Dr. Sanjay Bahl noted the key points such as the need for cooperation to build institutions and infrastructures and sharing of information to address the issues of cyber terrorism and cyber crime. There is a need for the BIMSTEC Member States to take a unified stand at the international forums. Additionally, he added, a database of perpetrators of cyber crimes could be managed and blockchain technology could be used for geo-tagging of malicious actors. The BIMSTEC Member States could also establish specific points of contact for sharing of information during emergency or crisis situation. He also drew attention to cooperation on both technical and law enforcement aspects, as BIMSTEC Member States prepare to take up more responsibilities pertaining to cyber security.

Session VII: Concluding Session

Chair: Maj. Gen. Alok Deb, Deputy Director General, IDSA.

Co-Chair: Pankaj Hazarika, Director (CS), BIMSTEC Secretariat.

Maj. Gen. Alok Deb noted the increase in cyber related crimes and attacks across the nation states and the importance of cyber security. He noted that the use of internet and smart devices has increased at a rapid rate in BIMSTEC Member States and that this will only grow in the future. Given that the Member States have common problems, they should have a common approach towards addressing them. He especially pointed out the misuse of social media and the spread of fake news as a common concern.

He stressed on the importance of adopting cyber-hygiene, training and awareness among people to reduce cyber crimes. A strong cyber security and privacy protection is a journey not a destination. He also spoke about the need to retain talent at the government level in the realm of cyber security to ensure a high capacity to deal with the emerging challenges. He stressed on the need of setting up of proper institutional mechanism and point of contacts for easier cooperation and coordination among the Member States.

- **Mr. Piyush Srivastava, JS (BIMSTEC), MEA**

  Mr. Piyush Srivastava extended his thanks to BIMSTEC Member States for their cooperation and noted how the coordination among them has increased steadily over the years. He highlighted the importance of BIMSTEC for India's

neighbourhood first policy and Act East Policy. He particularly noted the progress being made in the security domain, apart from that on economic, political, legal and other sectors. In this process, he noted the BIMSTEC home ministers meeting that focuses on issues of regional peace as well as the meeting of national security chiefs that has now become a regular feature. He said that Bay of Bengal is now recognized by the Member States as a common security space that has been expanded to include cyber security within its realm. He also spoke of the need to prevent misuse of cyberspace by terrorists and other rogue elements by adopting new strategies.

- **Concluding Address, Dr. Gulshan Rai, National Cyber Security Coordinator, Government of India.**

Dr. Gulshan Rai, in his concluding address complimented BIMSTEC secretariat, MEA, IDSA and all the Member States for meeting to interact on the issue of cyber security. He noted that while the penetration of Internet, mobile phones and ICTs is still lower as compared to other regions of the world, it is steadily rising. With its benefits also come problems like cyber attacks, with the financial sector being especially vulnerable. He predicted that in the future critical information infrastructure will face similar problems with the attacks steadily becoming more sophisticated. Especially with the huge amount of digital transformation and setting up of smart cities, he noted that a holistic approach is needed to address a convergence of issues that encompass legal, law enforcement, R&D, capacity building as well as norms for responsible state behaviour in cyberspace.

He said that as BIMSTEC countries need development for their economic and social growth, they will have to look at how to safeguard their interests in cyberspace. Though each country has its own rules and regulations, threats like these are known to transcend borders.

Hence, the next step in the process would be to ensure capacity building, R&D and CERT to CERT cooperation to share information and expertise. He recommended BIMSTEC to become a single unified voice of the region. He also suggested that MEA may consider setting up a forum that would meet on a regular basis on cyber security at the level of BIMSTEC.

- **Co-chair: Mr. Pankaj Hazarika.**

  Mr. Pankaj Hazarika noted the various important issues discussed during the workshop, namely:

  - To respect diverse culture of BIMSTEC countries and their sovereignty;
  - In the light of increasing internet penetration, understanding each countries capacity as well as vulnerabilities;
  - To build amechanism for effective intelligence and information sharing;
  - Importance of setting up nodal point of contacts;
  - To enable effective public-private partnership;
  - Importance of lab to lab cooperation;
  - To set up regional innovation hub indigenisation;
  - Importance of development of common standards;
  - To take a united position in international arena;
  - To chart out agreeable legal and institutional provision; and
  - To enhance capacity building.

  He spelt out various existing BIMSTEC mechanisms regarding cyber security, highlighting in particular, project based cooperation in technology agreed under Bangkok declaration and the working group on IT and communication related matters that will also deliver on cybersecurity. He noted that several initiatives on IT and cyber security are being undertaken, especially in the case of financial sector to share intelligence. He also proposed the idea of setting up a BIMSTEC Cybersecurity Center of Excellence, using existing infrastructure.

Roadmap for BIMSTEC Cyber Security Cooperation

Noting the importance of information and communication technologies (ICTs) as an instrument of social and economic development and as a key enabler for sustainable development,

Expressing concern over growing cyber threats, including threats to critical information infrastructure,

Taking note of the increasing malicious use of ICTs, both by state and non-state actors,

Underlining the need to bolster coordination and cooperation among BIMSTEC countries in strengthening security in the use of ICTs,

Acknowledging the need for international cooperation on cyber security amongst all the stakeholders,

Taking into account the UN Group of Governmental Experts (UNGGE) reports of 2013 and 2015, that international law, and in particular the UN Charter, is applicable to the use of ICTs by States,

Highlighting the need for development of confidence-building measures (CBMs) and capacity building in different areas of cyber security,

Participants of the 2018 Workshop on Cyber Security Cooperation for BIMSTEC Member states at New Delhi discussed and agreed on the principles of the Roadmap for BIMSTEC Cyber Security Cooperation to further strengthen regional cooperation on security in the use of ICTs as under:

- Develop mechanisms for sharing of information on cyber threats, malware and cyber incidents.
- Identify areas of cooperation in various aspects of cyber security, including capacity building.
- Establish a BIMSTEC CERT-to-CERT cooperation mechanism.
- Share experiences and best practices for the protection of critical information infrastructure.
- Strengthen law enforcement cooperation to address cyber crime, cyber terrorism and cyber security.

- Develop a BIMSTEC perspective on international cyber issues such as Internet Governance, Cyber Norms, data sovereignty, data protection, privacy.
- Work together on developing voluntary norms of responsible state behavior in cyberspace, to ensure an open, accessible, secure, stable, peaceful and equitable ICT environment.
- Encourage cooperation among stakeholders including government, private sector, civil society and academia for exchange of expertise, joint research, workshops and seminars.
- Promote capacity building and skill development in the areas of cyber security.
- Hold BIMSTEC Cyber Security Workshop annually on voluntary and rotational basis, as a regional forum to discuss various aspects of cyber security cooperation.

Annexure I

List of Participants from BIMSTEC Member States:

BIMSTEC Secretariat

Pankaj Hazarika
Sumon Kumar Shill

Bangladesh

Md. Sakhawat Hossain
Rehana Parvin

Bhutan

Sangay Choden
Sonam Choki

Myanmar

Kyi Khaing
Soe Naing Oo

Nepal

Khagendra Prasad Rijal
Rabin Basnyat

Sri Lanka

Dilan De Zoysa Siriwardana
Rohana Palliyaguru

Thailand

Rawinnipa Karin
Werachai Prayoonpruk

Published by:

Institute for Defence Studies and Analyses,
1, Development Enclave, (near USI), New Delhi, Delhi 110010
Email: iccoe.idsa@gov.in
Phone: +91-11-2671 7983 [Ext. 7221/7335]