



The Global Dialogue Security Summit 2021

Managing **CYBERSPACE** In the **INDOPACIFIC**

Date – Wednesday/Thursday, November 24/25, 2021 Venue – Shillong, Meghalaya

**GLOBAL DIALOGUE FORUM
&
THE INDIA OFFICE OF THE KONRAD ADENAUER STIFTUNG**

Present

The Global Dialogue Security Summit 2021

Managing Cyberspace in the Indo Pacific

Date: Wednesday/Thursday, November 24-25, 2021

Venue: The State Convention Centre, Shillong, Meghalaya

Mode - Hybrid

INDEX

1	The Report	Page 3
2	Preamble	Page 26
3	Schedule	Page 28
4	Curriculum Vitae	Page 32
5	Social media	Page 39
6	Photos	Page 45
7	Media Coverage	Page 56
8	About the Partners	Page 61

Written and edited by:

Ms. Nisha Ramdas, Director, Global Dialogue Forum

Ms. Inayat Naomi Ramdas, Assistant Director, Global Dialogue Forum

The fourth edition of the Global Dialogue Security Summit (GDSS) organised by Global Dialogue Forum (GDF) and the India Office of the Konrad-Adenauer-Stiftung (KAS) kicked off on Wednesday, November 24, 2021, watched by a worldwide, online and physical audience at the State Convention Centre, Shillong, Meghalaya, India. The conference was held amid celebrations of the 50th anniversary of Meghalaya's founding.

The theme "Managing Cyberspace in the Indo Pacific" found resonance amidst the COVID-19 pandemic, a shift in global perceptions towards China – a controversial actor on the world stage – and growing multilateral cooperation in the region.

Over two days, the hybrid conference discussed and analysed through experts in varied facets of cyberspace, with the speakers weighing the civilisational consequences of issues — from security to the environment to the economy to international law to technological advances.

GDSS 2021 had a total of eight sessions, featuring a glittering array of speakers including the Hon'ble Chief Minister of Meghalaya, Mr. Conrad Sangma. The speakers, present physically and virtual, examined the consequences — both good and bad — of the revolution in cyberspace that is taking over all aspects of human life and shaping a future world over this century.

The conference began with an introductory speech by Mr. Moses Manoharan, Chairman, GDF, affirming the theme of the conference whose focus was cyberspace and the Indo Pacific - two ideas whose time has absolutely come. Cyberspace, the "fifth frontier", with its threats and opportunities presents a new world order, one that was previously determined by a dominance of air, water, land and space.

Addressing the audience, Mr. Manoharan noted that GDSS 2021 had a host of glittering experts on cyberspace and the Indo Pacific, adding that Shillong could "claim its rightful place once again as not just a tourist destination, but a knowledge centre for young people".

Next, Ambassador Ruchi Ghanashyam IFS (Retd) was called upon to give an Indian perspective of the theme of the conference. She gave a brief overview of cooperation in the Indo Pacific and India's official stance there.

"It is only in the last decade that the term 'Indo Pacific' has gained prominence in the diplomatic and security arena, and became recognised as a geopolitical concept," she said.

Referring to the multilateral strategic cooperation, she pointed out the timely revival of the Quadrilateral arrangement called the QUAD, comprising the US, Japan, Australia and India spearheading the coalition emerging in this new geopolitical hotspot.

She further expanded on India's official stance on the Indo Pacific as highlighted by Indian Prime Minister Narendra Modi in 2018, outlying the national vision on the Indo Pacific.

"An open, stable, secure and prosperous Indo Pacific region was at the heart of this speech. In 2019, an Indo Pacific division was created within the Ministry of External Affairs," she said.

Ambassador Ghanashyam also quoted the Indian foreign minister saying that the India Pacific region reflected the reality of globalisation the emergence of multipolarity and the benefits of rebalancing.

She also brought attention to the various cyberspace strategies being developed by many countries including China.

The next speaker, Mr. Peter Rimmele, Resident Representative to India, Konrad-Adenauer-Stiftung, took the stage to give a European understanding of cyberspace and the Indo Pacific.

He started by stating that advances in IT and the decreasing cost of computing have created opportunities of using technology for the benefit of entire humanity, however there were many dangers associated with this as well.

Germany has also been affected adversely by cyber warfare, he said. "According to a recent study by the German Federal Association of Information Technology, in telecommunications and multimedia, there is hardly any company in Germany that is spared from cyber-attacks that are currently causing record losses of EUR 230 billion per year in Germany alone," he said.

It was more alarming that cyber-attacks were targeting the heart of democracies – the parliaments, he said, noting the case of the 2015 German parliament cyberattack. The media also feared that critical leaked information from this attack was used to influence voters in the 2017 German federal elections.

He warned that the world was at the cusp of an invisible war in which cyber vulnerabilities and critical national infrastructures pose severe threat to society.

"We also have to look into the ability of the cyber attackers to mask their identities and project a source of attack as originating from different identities, thus adding a dimension of geostrategic backdoor warfare," he said.

Mr. Rimmele also cautioned that the cyberspace neighbourhood was an area without geographical borders. For cyber issues and attacks, the entire world is a platform and attribution is a major challenge, he mentioned.

As for democratic values, he stated that cyber security is about defending shared values of democracy. Cybersecurity today is tantamount to defending our democratic way of life, freedom of speech, he added.

"Cybersecurity is about defending these shared values that we hold dear. It's not only about technical issues, it is about defending our free and open societies. Both the EU and India face similar cyber threats. So it has become imperative that we develop a converging approach between our like-minded democracies to counter them and halt them from undermining our rules-based international system," he said.

Mr. Rimmele also recalled joint initiatives like the EU-India Digital Connectivity Partnership which has sparked discussions on convergence of regulatory frameworks to ensure a high-level of protection of data and privacy.

“This represents a cornerstone for the formation of globally harmonised data protection standards which are imperative in view of the exponentially growing numbers of cyber-crimes around the world,” he noted.

He commended the EU-India Summit in May 2021 but said it was important that the EU and India crafted a joint strategy or joint cooperation to deal with the ever emerging cyber challenges.

Next, the Keynote Address was delivered by Lt. General Rajesh Pant. PVSM, AVSM, VSM (Retd), India’s National Cyber Security Coordinator. Lt. General Pant opened his address by alluding to a few lines of Rabindranath Tagore’s *Gitanjali*, “where the mind is without fear and the head is held high”. He said, “this is what we want cyberspace to be: safe, secure, trusted, resilient, vibrant and something that contributes to national security”.

Cyberspace is a global common much like the climate, environment, pandemic, he said adding that global commons require global solutions.

“As far as this particular year is concerned – 2021 – in the cyber front, there is both good news and bad news. The good news is that internationally a lot of collaborations are coming together,” he said, referring to the concerted efforts at the UN and multilateral levels (e.g. QUAD) in establishing norms for responsible behaviour by states in cyberspace. “The bad news is cybercrime. The World Economic Forum has called cybercrime as the biggest man-made risk to economic progress,” he enunciated, adding that in 2020, there was a loss of six trillion USD to cybercrime.

Lt. General Pant also said healthcare was a highly targeted industry for cybercrime in India because of the vulnerable data it contained. Supply chain attacks are on the rise as in the case of the SolarWinds hack which affected 18,000 companies.

“The digital transformation due to COVID has really widened the attack surface,” he stated. Attribution of cyberattacks is a worrisome issue, said Lt. General Pant. Over 40 per cent of the attacks seem to have emerged from the US mainland. However, attackers use a series of sophisticated “hops” to conceal their locations, thus the large attribution to crimes originating in the US, he said. More than often, these “hops” are countries with strict privacy laws which will not allow the revelation of Virtual Private Networks (VPNs) employed.

The speaker then turned to the Indo Pacific, a region “increasingly being viewed as a global centre of gravity”.

“India is the champion of a free and open Indo Pacific that was mentioned. It is engaged with its partners in the region, such as under the QUAD mechanism, to ensure the rules, norms and standards that govern new technologies reflect our vision of free, open, resilient and inclusive Indo Pacific,” he said.

Lt. General Pant referred to the meeting of the QUAD countries earlier this year to reaffirm their commitment in the Indo Pacific.

“The focus of the Indo Pacific is therefore on connectivity and answering maritime security, counter terrorism, non-proliferation and cyber issues. For managing cyberspace in the Indo

Pacific, we need to define our commitments based on shared values and priorities, which play a greater role for the security and stability of the region's maritime domain," he noted.

"India is already on the path of implementing existing legislations and legal frameworks to safeguard the national sovereign cyberspace," he said, adding India's national cybersecurity policy and IT Act were under review. He said that the Indian government is also working on a national cybersecurity strategy.

Lt. General Pant then said that action needed to be taken to enable development of a sound ecosystem supplementing the three pillars of securing national cyberspace, strengthening our existing structures and synergising resources for their optimal utilisation. "Out of all the critical sectors, two are super critical. So, presently, we are laying a great focus on the telecom and power sectors because they underline all the other sectors," he said.

To conclude, Lt. General Pant reiterated that cybersecurity is about collaboration and advocated for a strong coordination between global, regional and federal organisations along with Public Private Partnerships (PPPs).

"This will not only help us to counter cybercrime, but also pursue new areas of innovation, digital economy, cybersecurity and cyber-enabled critical and emerging technologies," said Lt. General Pant.

This was followed by **Session I: Defining Cyberspace and Identifying its Challenges**. It was chaired by Major General Lav Bikram Chand, VSM (Retd) from the Corps of Signals of the Indian Army.

The chair laid down the foundation for his session on "cyberspace and identifying its challenges". He began with a reference to China's new status as leaders in cyber technology, the dependence on cyberspace and how hackers too were vulnerable to attacks.

"The rapid evolution of cyberspace, evident by the increase in processing power & memory of computers and AI (Artificial Intelligence), poses challenges that need to be addressed. Cyberspaces' omnipresence rakes up privacy issues that must be addressed," he said.

He illustrated this with a reference to a joint venture of British Telecom and Huawei, a Chinese tech company which led to two conclusions – in the race for commercial productivity vulnerabilities took a backseat and version compatibility could not be guaranteed.

Challenges arise when one talks of infrastructure, he said. "The 5G conflict brings many issues as billions of windows are open to come into cyberspace. The distrust of software by users has led to private clouds which could fall prey to a malicious malware which could prove to be a nightmare. Hence, security management becomes important," he said.

Maj General Chand ended with a quote, "Future conflicts are no longer going to be won by using cyberspace and electromagnetic spectrum, but rather they will be won by cyberspace and electromagnetic spectrum."

The first speaker of the session, Vice Admiral Professor Dr. Ir. Amarulla Octavian, S.T., M.Sc., DESD., of the Indonesian Navy, Rector of the Republic of Indonesia Defense University, joined the conference virtually from Jakarta, Indonesia.

Vice Admiral Octavian highlighted the importance of cyberspace in the Indo Pacific region. "Indo Pacific is a very dynamic region, both in the present and the future. Several countries in the region such as India, China, Japan and others are economic powerhouses that can contribute positively to improve the global welfare. On the other hand, national interest of countries in the region and their interaction with the interest of superpowers beyond the region also play a key role in maintaining and safeguarding the security stability including the effort to deal with cyber threats."

He further noted the border contestation amongst nations of the region and the Indo Pacific also being a region vulnerable to transnational cyber-crimes.

He moved on to cite the rapid growth of AI and Big Data which has affected all aspects of human life including military and defence which had led to the emergence of the Second Wave Revolution in Military Affairs.

Showing a concern, he went on to say that "Global and regional security also has the cyber space dimensions beyond the real world dimensions." He pointed out that cyber threats were imminent and needed to be addressed immediately for which new military technology was required to deal with cyber-crimes.

Military technology advancement in the use of unmanned systems had led to the creation of robots capable of performing technical functions similar to human soldiers with high reliability to work accurately under any condition, he noted.

The speaker said that cyber technology could be used effectively to reduce the number of military soldiers, and it could accelerate weapons acquisition and procurement process at every stage. It would be able to cut logistics chain length while ensuring sustainability. "Cyber technology improved the accuracy of surveillance and recognition process. At the same time, denial and prevention process could also be carried out through cyber technology. It has been developed for prioritizing cyber security for command and control and the supporting devices of the sensor and weapons systems," he said.

He mentioned that many militaries were developing non-fuel technologies for reliable military performance; the cost of establishing these was high but the maintenance and operating cost were reasonable. "Cyber technology is able to reduce waste as in the case of automation as all data and information does not need to be printed on paper. The use of new and renewable energy on all military platforms could reduce pollution and Green House Gases (GHG) emissions," he said.

Vice Admiral Octavian concluded that emerging technologies in cyber domain could develop faster and more exponentially in line with innovation and creativity in the use of AI and Big Data. "Threat trends in cyberspace had emerged with the use of emerging technologies by state actors, non-state actors and/or state sponsored actors. As the nature of cyber threat is transnational, it could be best dealt with joint efforts," he said.

A cyber-attack on one country was likely to affect the system in another country or region. The Indo Pacific region with its various potentials and opportunities to develop new technologies in the cyber domain, would have to take into account cyber security vulnerabilities, he stressed.

The second speaker of the session was Mr. Md. Nobir Uddin, Senior System Analyst, ICT Division, Ministry of Posts, Telecommunications and Information Technology, Government of Bangladesh.

Mr. Uddin's presentation on Digital Bangladesh began with a mention of a number of initiatives that were underway. The government, in its attempt to digitalise Bangladesh and connect people, is working towards developing human resources, promoting industry with e-parks, etc. and encouraging a start-up ecosystem.

He mentioned the working of the Bangladesh e-GOV CIRT (Computer Incident Response Team) with the Digital Security Agency where the latter takes on the responsibilities of the National CERT (N-CERT). So far 4550 incidents of cyber-attacks have been reported and CIRT is with 278 government organisations.

The government has identified 28 Critical Information Infrastructures (CIIs) that includes financial institutions and the Taxation Department.

Bangladesh is taking several initiatives to ensure Data and Information infrastructure protection. Among the various initiatives to bring appropriate training for the youth, the government had started cyber skill programmes and Cyber Drill.

To protect the information structure, a strategy known as Bangladesh Cybersecurity Strategy guidelines have been formulated. Other worthy steps have been taken to mitigate future cyber risks: A Cyber Range established in 2019 to train cybersecurity professionals, a Capture the Flag (CTF) to assess capability of cybersecurity force and organised a Cyber Drill 2020 for Financial Institutions.

All these deliberate steps have seen Bangladesh reach the 41st rank in the Global Cybersecurity Index and is on the top position amongst SAARC countries in cybersecurity.

Mr Uddin further spoke on the CIRT's other activities with respect to the military and visits to their centre by other government officials of other countries. He ended with a mention on the international cybersecurity collaborations, for instance Asia Pacific Computer Emergency Response Team (APCERT) and Norway Registers Development (NRD).

Mr Uddin recognised the role of both India and the US in creating widely used digital products. He noted how the internet had played a role in the growing economy, military competition and asymmetric warfare and diplomacy and trade in the Asian region.

He also spoke on the need for digital hygiene as a necessary requirement for cybersecurity. He enumerated many "non-electronic" attacks – shoulder surfing, dumpster diving and social engineering as becoming prevalent.

The final speaker in this session was Brigadier Ashish Chhibbar, Senior Fellow with the Strategic Technologies Centre at the Manohar Parrikar Institute for Defence Studies and Analyses in New Delhi. He spoke on India's cyberspace capabilities.

His presentation covered three main areas: what does one mean by Artificial Intelligence (AI), what are its discernible trends especially for nation building, and major recommendations.

He elaborated that AI can do tasks that were earlier impossible. "They are autonomous machines which do not need any external input. These intelligent machines will perceive their environment are capable of self-learning. The good results are on their own without any external inputs," he said.

He elaborated on the ways AI is different from a standard computer. "Standard computer manipulates a set of known inputs to produce an output and this output will always be the same for the same inputs whereas AI produces different outputs," he said.

A programmer for a computer knows the number of steps that leads to a particular output. "In the case of AI, it is the opposite: AI does not know how the information has been processed. AI gives workable solutions," he explained further.

Brig Chhibbar explained the three stages of training, learning and testing, that AI goes through for its output. "The prerequisites required by AI are clean and annotated data, algorithms, and large amount of data. AI goes through self-learning and several iterations before it starts giving the desired results," he said.

Brig Chhibbar also informed the audience of the shortcomings of AI. "If the data is not large or clean, it can prove to be stumbling block for AI," he said. "Amazon did away with their own hiring software because that software became very biased towards men than women."

He spoke on the black box syndrome and mentioned that AI machine could only solve one problem. It would be at least 30 years before a general AI machine would be ready.

Brig Chhibbar stressed on the importance of ethical norms and standards when it came to AI.

"India has been among the foremost leaders in this aspect. In February 2021, the NITI Aayog laid down seven principles of responsible AI. In August 2021, it laid down actual ways of making these operational," he explained.

He then spoke of India's potential in AI. India has the highest AI skill penetration in the world, he said adding that AI-specialist was the second emerging job role in India in 2020. AI has deep economic benefits and many of the largest AI- based industries are education, finance, hardware and networking. Many tech start-ups in India use AI technology.

Brig Chhibbar said that AI has the potential to add USD 400-500 billion to the world economy by 2025. Forty four per cent of deep tech start-ups in India leverage AI technology. AI investment in 2020 was maximum in drug design and discovery (because of the pandemic).

Most industries have AI working in the backend. "If you hear intelligent and smart, be reassured that there is an AI software or AI algorithm working in the back end generating inputs from the data," he said.

As for recommendations, he suggested that R&D and innovation should be rewarded, data centralisation should be made a priority, high speed internet connectivity is needed to monetise India's generation of large data. He also said that India needs to promote "Make in India" and "Code in India".

In session II - **Collaboration and Conflict over Cyberspace in the Indo Pacific**, its chair, Lt. General Arun Kumar Sahni, PVSM UYSM, SM, VSM (Retd), the former General Officer Commanding in Chief, South Western Command, said that dependence on cyberspace was growing exponentially.

"With this kind of dependence, there are vulnerabilities being created which are exploited," he said. "It is very important that we understand where and how we can ensure our security and the safety of our infrastructure."

Lt. General Sahni expressed concern over the security of the financial sector's Critical Information Infrastructure (CIIs) in the Indo Pacific region which had become the *de facto* financial centre of the world. "It is actually going to impact global economy," he said adding, "So any denial of this is going to be an area of extreme concern to each and every one."

He also stressed that China's impact was to be taken into account when discussing cyberspace and sovereignty in the Indo Pacific.

Various elements of cyberspace had been harnessed by China and the People's Liberation Army (PLA) Strategic Support Forces, he stressed, charging that Beijing was at the heart of many ethically questionable activities. But it was nevertheless a key player in cyberspace, he acknowledged.

Lt. General Sahni also noted the collaborative efforts of South Asian regional forums like the ASEAN and the ASEAN Regional Forum (ARF), which were deeply concerned with developments in cyberspace and cybersecurity in the Indo Pacific. Other multilateral organisations like BRICS (Brazil Russia India China South Africa) and the Bay of Bengal Initiative for Multi-Sectoral Technical and Economic Cooperation (BIMSTEC) were also preparing to address this sector and its challenges, he added.

The next speaker, Mr. Amit Sharma, Advisor (Cyber) and Director in the Office of the Secretary Department of Defence (R&D), spoke on cyber warfare and its contemporary challenges, highlighting three aspects: Cyber Crime, Cyber Terrorism and Cyber Warfare. While cyber warfare was the most sensitive of them all, all the three exchange hands quite often. "Cyber warfare is a realm that is primarily in the domain of state actors," he said.

The post-2004 world had seen states investing heavily in cyber warfare. "In time, states and companies also invested in securing their assets," adding that states were now anteing-up on both ends.

Mr. Sharma equated cyber weaponry with traditional military weapons like missiles. Components like viruses and malware worked like weapons because of the elements of precision and stealth and a high level of targeting accuracy, very similar to military weaponry.

Mr. Sharma then elaborated on various kinds of cyber weapons and incidents in which they had been used recently in Estonia, Georgia and Ukraine among other countries. He also said that confidentiality was under threat from data extraction.

Mr. Sharma also noted that current challenges in cyberspace included Advance Persistent Threat (APT), hi-tech AI assisting assault, the containing of data within geo-boundaries, sovereign control over digital infrastructure and prevention of Weaponizing of Tech Giant (WTG).

“We can only achieve a strong cyber defence system if we have global and collaborative leadership in technology,” he stressed.

The next speaker Dr. Geoff Heriot joined in virtually. Dr. Heriot, Member of the Council of the Tasmanian branch of the Australian Institute of International Affairs, one of Australia's oldest think tanks, focused on conflict and national sovereignty in cyberspace. He started his address by giving an Australian view of developments in cyberspace.

For Australia with a comparatively small population, self-sufficiency in technology or in critical supply chains was unlikely. “So, collaboration for Australia is essential if it is to retain agency in the cyberworld,” he said.

Dr. Heriot commended the success of the Sydney Dialogue that took place in India in November 2021. The dialogue, an initiative of the Australian Strategic Policy Institute in partnership with the Australian Government, included leaders like Indian Prime Minister Narendra Modi, his Australian counterpart Scott Morrison, former Japanese Prime Minister Shinzo Abe, former Australian Prime Minister John Howard and Indian and Australian foreign ministers. He said that the Sydney Dialogue was a step forward in the Australia-India relationship in the Indo Pacific.

“This new initiative is also concerned with issues of cyber technologies, their strategic significance and that of other critical and emerging technologies,” he said.

Australia had in 2008 already identified e-security as a key priority but the government’s activities could barely keep up with those of hostile actors, he noted.

“Since then, fortunately, the government’s amble has become a sprint. I think it is highly unlikely that the pace of engagement would slow even if next year – when we are scheduled to have general elections – there were to be a change in government,” he said.

Apart from policy developments, official efforts were being made to make clear the opportunities and risks in cyberspace, he added. Australia, he said, had strong expertise in Quantum Technology, that could prove significant in cyberspace.

Dr. Heriot spoke at length on the role of the QUAD and other minilaterals in cyberspace in the Indo Pacific. Australia was a small partner in these organisations but demonstrated a willingness to contribute, he said.

Dr. Heriot highlighted three attributes of these organisations: long established friendships which enabled joint problem-solving abilities, facilitation of new relationships with other

prospective partners, and existence within parallel and larger formal frameworks and alliances.

Although critical of the newly formed AUKUS, he said it had a role to play in the Indo Pacific. He brought to attention that Japan under former Prime Minister Shinzo Abe, had expressed a willingness to collaborate with such allies in the Indo Pacific.

Dr. Heriot also spoke of the ethical and reputational dimension of the cyber challenge – “a dimension on which so much depends for those nations who proclaim democratic principles.”

“One argument put forward recently is that the democracies remain still fundamentally unprepared for strategic competition with hostile actors in this information age,” he said. “One defensive bulwark relies on the degree to which citizens have a reasonable degree of trust in government, in their public institutions and society,” he said.

The next speaker, also joining the summit virtually, was Mr. Alok Sinha, CEO, Globus Eight Inc. He listed current dangers that players face in cyberspace including Advanced Persistent Threat (APT) by state and non-state actors.

“Allegedly, offensive capabilities are very advanced for six countries – they are called the Big Six – China, US, UK, Israel, Russia and North Korea,” he said, adding that they had the capabilities to launch APT action items. India is still at a stage of evolution when it came to capabilities in the APT space.

For the industry, the major concern remains internal and external safety measures or what he called ‘scaffolding’. The world of coding needs to have a more adversarial security approach. AI-assisted assault was a cause of concern too what with its low-cost and high accessibility. Another concern was the containment of data within the geographical boundaries of a state.

Mr. Sinha also pointed to a key piece of hardware which he called new face of cyberspace. Semiconductor chips which are used in all modern electronics and are enabling the rise of AI and the Internet of Things (IoT) are becoming faster and cheaper.

The hindrance of supply chains due to the pandemic, a trade war between the US and China and the Taiwan drought caused a shortage of this hardware which had adversely affected the supply of this component. He also highlighted the issue of securitising supply chains.

Mr. Sinha concluded by saying, “as long as technology evolves, we will also have to evolve in a collaborative manner”. No one nation can survive in isolation, there is a need for ‘trust partners’ he added.

In **Session III, Cyberspace in Industrial Development**, the chair, Ambassador A.R. Ghanashyam IFS (Retd), India’s former envoy to Nigeria, and alumnus of Indian Institute of Management, Ahmedabad laid out the contours of discussion, tracing the evolution of computers and illustrating the growth of the sector through numbers. In 1995, 0.4 per cent of the world was internet-enabled, and this grew to 64 per cent in 2020, he said.

Ambassador Ghanashyam drew attention to the simultaneous growth of data, 90 per cent of which had been created after 2016 . He said that in India, data protection was very much part of cyberspace over which cyber-attacks were growing. He put forward figures of the origin of cyberattacks in India.

“In India in 2019, we had 400,000 cyber-attacks on various institutions of India. In 2020, we had 1.1 million cyberattacks. The calculation is that 28.6 per cent of these attacks originated in China, 28.6 per cent came from Pakistan, 7.1 per cent came from North Korea and 35.7 from unknown sources,” he said.

He then introduced briefly the three speakers in the session and invited them to speak.

The first speaker was Professor Heribert Dieter, Economist from the Stiftung Wissenschaft und Politik, the German Institute for Security and International Affairs, in Berlin, Germany. He based his address on what cyberspace meant for economic and industrial development.

“One could argue that the days of limited importance of political and security matters in economic and industrial development are over. Whatever is done in the economic domain is analysed and observed from a political angle and today we’re not just talking about profits, about investment, about benefits of international division of labour, but we are also looking at the geopolitical conflict that is increasingly shaping international economic relations,” he argued.

Professor Dieter then said in cyberspace, the shared use of knowledge is difficult. There is a greatly diverging perception of ownership of data. Just because data is available does not mean we know what to do with it, he argued. He said new technologies were not being shared with China in the same way as with the erstwhile Soviet Union.

He went on to highlight issues with the economies of Germany, China, India and the US, arguing that while the former two had a declining and aging workforce, it was the opposite for the latter two countries.

China’s use of technology – specifically robotics – was an outcome of a rapidly aging and increasingly expensive workforce. “China has priced itself out of the market in a number of sectors,” he said, warning of 25 per cent decline in workforce by 2050.

“Wages are up, labour supply is down. The Chinese answer is robots, a response to challenges of the labour market. Alternative for China would be to embrace immigration – in theory that is possible but in Xi’s China, immigration does not play a major role and the leadership has no intention to embrace the EU/US immigration policy to support the declining workforce. They have a preference for political stability and they are willing to pay a price for it,” he said.

Professor Dieter said that although Germany had the same issue with workforce, the reaction was opposite in that the use of robots in industry is “evolutionary rather than revolutionary”. India, on the other hand, was well placed for cyberspace industrial development due to its large, young work force.

He also cautioned that if the cost of maintaining a safe cyberspace was too high, development would most likely slow down or end.

The next speaker was Mr. Ravi Nirgudkar, Managing Director, BAE Systems – India. His address provided an industry perspective on the conference theme and stressed that the risk of cyber threat was of great concern to corporates including his own.

“Cybercrime is third behind corruption and narcotics as the global economic problem. The cost of cybercrime is close to one percent of the global GDP, risk to cyber security is increasing in number & severity. 50 percent of industry today do not have a good cyber security plan. What is required is a good cyber security strategy and cyber security crisis management plan,” he argued.

He said that though cyber security was the responsibility of IT staff in a company, it nevertheless required commitment, support and vision from the management. He underlined the necessity of a cyber security risk management plan in the corporate world.

“Cyber security risk management plan is a necessity. The plan is to have three parts: defensive techniques, recovery plan, an offensive. Defence techniques protect you from cyber threats, the recovery plan is what you develop when you get attacked and the offensive is to make sure it does not happen again,” he said.

He warned that a cyber security breach could result in loss of reputation, theft, financial losses, fines, penalties and the intangible feeling of insecurity.

Mr. Nirgudkar also listed many avenues in which BAE Systems was working to ensure cyber security in India, adding that their vision was a self-reliant India when it came to cyberspace.

The last speaker was Mr. Argha Bose, Head, Cyber Security, Tata Advanced Systems Ltd, who spoke on the why cyber security was crucial to industrial development.

“The convergence of the cyber and the physical worlds had opened the door to new vulnerabilities, centred on Industries relying heavily on connected technologies and software that included multiple stakeholders in the value chain. These created vulnerabilities through the drastically increased access points in networks,” he said.

Mr. Bose drew attention to the increasing number of cybersecurity attacks – citing the Triton malware attack, the Kudankulam Nuclear Power Plant attack, Stuxnet, U.S. Colonial Pipeline, among others.

His presentation also elaborated on how one could address the cyber security risks in industrial development by better understanding IT and operational technology, embracing a risk-based security model, identifying and fixing outdated systems.

Mr. Bose spoke about the importance of securing cyberspace while highlighting its effective outcomes and why industries need to have a proactive approach to optimise their future prospects by amplifying their cyber-defensive and offensive capabilities.

Day II began with **Session IV: Conventional War, Cyberspace and Sovereignty.**

Its chair was Lieutenant General Sunil Srivastava, AVSM, VSM** (Retd), Director, Centre for Joint Warfare Studies (CENJOWS). He opened the session by stating that there was a lack of consensus on the definition and understanding of the terms “conventional war”, “cyberspace” and “sovereignty” and went on to make observations about their broader understanding and scope. He noted that “war” had gained a wider meaning today – it alludes to coercive situations that involve both military and non-military actors with both violent and non-violent means.

“It’s no more a situation of relationships between states as if they are at war or peace. This kind of a binary understanding is not the kind of prism to be looking at wars and conflicts today. And it’s no more state versus state; there are non-state actors, there are irregular actors, private military companies involved and even civilians involved,” he said.

Lt. Gen. Srivastava noted that means of coercion had changed from being predominantly violence-based to more hybrid. All these conflicts remain below the threshold of war, are protracted and typically asymmetric, he added. In this context, cyber tools have great relevance.

“Asymmetric adversaries increasingly find the unique utility of these cyber tools which are affordable, available and they are equalisers. Cyber tools are very ambiguous in terms of their source, in terms of their intent and also in terms of their effect,” he said.

He then elaborated on the terms “cyber weapons” and “cyber domain” saying that the cyber domain is manmade and pervades and transcends all the other four – air, space, land and water. It enhances their effect at the tactical and operational levels of war.

He noted that it was important to make a distinction as to who used cyber weapons at war. “Unlike cyber terror and cybercrime, cyber espionage and cyberattacks require great sophistication in planning, reconnaissance, deployment, attack and finally withdrawal. And that entirely is a preserve of states,” he said.

Lt. General Srivastava then pointed out two challenges in the area of cyberspace and warfare. One is deterrence by denial which calls for a very strong cyber defence. The other is having early warning systems in place since cyber warfare gives no signs. He added that offensive weapons are a strategy of choice when dealing with such attacks.

He proceeded to list many dilemmas in cyberspace. What defines an act of war in cyberspace? What thresholds need to be crossed in terms of sensitivity, scale, etc. to justify the right of self-defence under Article 51? What would be the rules of engagement? What about the principles of humanitarian law, necessity, proportionality, distinction? How does one deal with escalation control?

Lt. General Srivastava said that it was imperative to discuss the role collaboration of private players and governments in the cyberspace domain.

On the international front, there was still a lack of consensus on international security dealing with cyberspace although there were reports like the UN's Open-ended Working Group's (OEWG) that gave recommendations on advancing peace in cyberspace.

He ended his address by questioning if cyber diplomacy is the only way forward. "The time to act is now if we want to prevent the cyber domain from becoming lawless," said Lt. General Srivastava.

The next speaker, Mr. K.P.M. Das, National Cyber Security Officer of Cisco India, joined the summit virtually from Bengaluru.

He addressed the issues of cyber states and cyber sovereignty. He said that cyberattacks have proven to be a low-cost tool for statecraft which can inflict great political and economic damage. "Because it is non-violent, the attention of the global community including citizens is very low, very short term. To my mind, doctrine is more important than settling on international laws," he said, recalling that while cyberspace and technology had developed over the last decades, checks and balances were still not up to the mark.

Mr. Das noted that distinctions needed to be made when it comes to conventional and cyber attacks regarding tangible structures and threats.

Talking about cyber states, he said, "I would call a cyber state one where the entirety of the state is dependent on cyber infrastructure – the government, the people, everybody. And that is a net positive in a peace scenario but it is not a net positive in a no-war/no-peace scenario," he said.

He added that cyber attacks have not yet reached the level of a cyberwar and therefore states have not yet considered them as a threat to sovereignty. "To my mind, we need to completely redefine what is sovereignty; a lot of it today is amorphous, it is fuzzy," he said.

Mr. Das added that international norms are based on international laws and cited the Geneva Convention, UN charters as examples. However, none of these apply to cyberspace. He recalled the example of Iran and the STUXNET worm attack during which time Tehran did not want to admit that the cyber attack had left its sovereignty threatened. International response has fallen short not because of national or international reasons but because of the nature of the problems caused by cyber attacks, he said. Therefore, doctrine needs to be examined.

Mr. Das also noted that cyberspace is more complex as actors are no longer limited to the nation state and involve a myriad set of state proxies and civilians. "We are in early stages of international talks on what constitutes cyber sovereignty and what is that thick red line which an adversary should not cross," he concluded.

The next speaker Mr. George Mikaberidze, Chief Executive Officer, Rosinfocominvest, Moscow spoke about digital colonisation and how cyberspace has aided loss of digital sovereignty of many states. He stressed that a state's digital sovereignty is a new but very important component of the sovereignty of the state.

“Digital sovereignty is a right and ability of a national government to first, independently pursue its international and geopolitical interests in its digital space; second, it’s to define its own independent internal and external information politics; third, it’s to defend and guarantee the cyber and informational security of the country and population; fourth, freely use the national resources and infrastructure,” he said.

He also spoke about the main elements of digital sovereignty, how to obtain them and how to achieve digital sovereignty.

Mr. Mikaberidze also warned of the digital colonisation taking place in many countries today. He highlighted many ways in which this is carried out by foreign actors (state and non-state) including loss of control over infrastructure (e.g. backdoors in software), possibility of economic and political pressure (e.g. control of social networks), degradation of own intellectual resources (e.g. overdependence on third-party players) and a digital tribute (e.g. constant deductions for software maintenance).

“If a country nowadays does not maintain its digital independence, it would eventually lose all other components of sovereignty (political, economic, military),” he said.

The next speaker, Mr. Shreyas Jayasimha, specialist in cyber and space laws, Founding Partner, Aarna Law, took the stage to highlight laws governing conventional warfare. He said that conventional war and the use of arms do not address several complications that come into the picture while discussing cyber arms.

Taking a cue from the earlier speakers, Mr Jayasimha asked if international law has turned irrelevant and if it was indeed the time to look beyond at a doctrinal approach towards cybersecurity. “Hopefully the pace of norm setting in the current context will not incur cyber Pearl Harbours,” he said.

Alluding to the UN OEWG’s eleven norms of responsible state behaviour in cyberspace he said, “it is with some effort that a consensus was reached at the UN platform and this is as good as we have. But there have been several attempts not just by states but by academics to try and pull together norms which could form the basis of future conventions.”

He pointed in particular to the Tallinn Manual an academic, non-binding study conducted between 2009 and 2012 on how international law applies to cyber warfare and cyber conflicts.

He also briefly spoke on the cryptocurrency regulations around the world. “There is a deep interconnection between the concepts of cybersecurity and cyber peace that have been discussed over the past few days as well as regulation of cryptocurrency in general,” he said, referring to a new bill on cryptocurrency which is set to be introduced in the winter session of the Indian Parliament. Mr. Jayasimha added that India is strategically placed to play a role of a synthesiser difference in thinking systems in cyberspace with initiatives such as NITI Aayog’s seven principles on AI.

The next session was **Session V: Cyberspace Connectivity for Peace and Development in India's Northeast**

The session was chaired by Hon'ble Member of Parliament Mr. K.J. Alphons, Member, Parliamentary Standing Committee on External Affairs. He opened the session by saying that it was very important to be connected to Northeast Indian states which is very often not the case because of its geographical distance from the centre of the country, however cyberspace has made physical distances redundant.

Mr. Alphons called attention to the fact that India has been in the forefront of developments in cyberspace. While Internet was once a luxury, it is not so anymore for the common Indian. He reiterated Indian Prime Minister Narendra Modi's agenda of connecting the whole country to the Internet via cyberspace.

"Indian talent plus information technology would be India's tomorrow. The benefit of the cyberspace must reach people," said Alphons, quoting Modi. "We need to use the opportunities which cyberspace offers. The Indo Pacific is the happening place now with growth meeting all areas but also has serious issues about security because some people tend to be a little more aggressive than other people."

Threats to individual freedoms, security, privacy remain concerns with respect to cyberspace in the Indo Pacific which need to be addressed, he said.

Mr. Alphons also spoke of initiatives by the Indian government to enhance connectivity in the country. He pointed to the Indian government's BharatNet initiative to provide broadband connectivity to 250,000 panchayats (local self-governing bodies) across 600,000 villages in India. "We have already laid optic fibre connections to about 175,000 panchayats. By 2023, every panchayat and village in this country will be connected to optic fibre," he said.

Another project under the Digital India Programme is the setting up of Common Service Centres (CSCs) across rural and remote locations that aide citizens in availing government services. About 375,000 such centres have already been set up, said Mr. Alphons.

Next, Dr. Pfokrelo Kapesa, Assistant Professor, International Relations, Northeast Christian University (NECU), Dimapur, Nagaland took the stage to talk about pitfalls and challenges of cyber connectivity in Northeast India.

She said that the COVID-19 pandemic has exemplified the importance of cyber connectivity especially in the education sector and for small businesses. "However, the challenge of connecting a very large number of people especially in the far-flung regions like Northeast India continues to remain. The connection to digital networks does not only impact the ways individuals and society operates, the way businesses operate but it plays a very important role in the relations between the government and citizens," she said.

Dr. Pfokrelo stressed that a major concern in the Northeast is the emergence of new societal vulnerabilities, a result of technological leapfrogging. "We do not have systems in place, mechanisms in place and yet the use and dependency on cyber connectivity has increased so much without proper regulatory and governance mechanism," she noted.

Instead of being a positive change, cyber connectivity has created new vulnerable sections of society, a concern for Northeast India which comprises of over 200 multi-ethnic communities. She brought light to the fact that over 90 per cent of the area in Northeast India is international border land and the region has not been a stranger to long cycles of conflict.

“The society that we see in the northeast today is highly fragmented and volatile at the same time. Cyber connectivity and digitisation can in many cases empower communities to resist violence, provide avenues for alternative discourses to engage with each other but can also become a source of conflict especially for a region that has a lot of conflict faultlines and cleavages,” she said.

Dr. Kapesa also spoke on data manipulation by organisations and actors. “For a region, for people who have seen a lot of conflict and upheavals, access to cyber connectivity and increased rate of digitalisation that we see today is not only about compromising privacy but it can become a pertinent threat to individual security,” she said, adding that cyber connectivity can have two faces. While on the one hand, cyber connectivity has helped efforts in conflict resolution, many have used it to spew hate and encourage violence. She cited the example of a bulk circulated Whatsapp message in 2018 on suspected child kidnappers which had led to their lynching.

She ended her speech by stressing on the importance of dialogue between the citizens of the Northeast, leaders and policymakers to create comprehensive, vibrant and inclusive cyber regulatory mechanisms that can harness digital connectivity to promote peace and development in the region.

The next speaker to take the stage was Mr. Mutchu Mithi, Hon’ble Member of the Legislative Assembly, Roing, Arunachal Pradesh. Mr. Mithi began his address in a humorous fashion by narrating an example of a digital relationship between spouses, alluding to what cyberspace meant to the common man. He then went on to say that information and data is no longer confined to the privileged few.

“After the advent of commercial airlines, cyberspace has been a humongous leap for mankind, also for the nation and also for my state, and also for the region as a whole. This is science-fiction in reality. It opens doors to new dimensions, new galaxies, new opportunities, new frontiers where we have never trod before. So, there is huge opportunity in cyberspace,” he said.

Mr. Mithi enlightened the audience on how cyberspace has altered governance in Arunachal Pradesh by citing an example of the recruitment process of officials. There were many rumours of unethical procedures in the state’s recruitment process in 2020. However, certain evidence of such foul play was noticed by government officials on social media after which the necessary investigation was undertaken and culprits were caught. The result has produced fear in officials and thus a more ethical recruitment process.

Mr. Mithi went on to speak on racial discrimination and cyber connectivity in Northeast India. “To the people of Northeast, racial discrimination still exists but it has largely subsided. And how has it subsided? Not by government interventions but by awareness, by knowledge,” he

said, adding that many potential and former perpetrators are now fearful of backlash. “So, the Internet has also changed our behavioural patterns”.

Furthermore, he noted that the Northeast has a huge problem in connectivity. “My constituency borders a district that is bordering the Indo-China border. There are so many constraints while accessing people,” he said. He also recalled the 1962 Indo-China war where Arunachal Pradesh was the first line of defence to the Chinese aggression. “Now what we see is that with the lack of internet connectivity, there is a huge migration going on – migration from the border areas to nearby towns. This is also a security concern for us that the governments of the day should think about,” he said.

Mithi noted that the Internet had given a voice to the people of the Northeast, not only in individual terms but also as a collective. India has an ever-increasing number of subscribers to Social Media platforms and it was important to know how to deal with it, he said.

In conclusion, Mithi noted that cybersecurity was a serious issue and cyberspace can be misused. “But just because something can be misused doesn’t mean that we cannot use it. The guardrails are being put in place and have been put in place but since these are new dimensions, these are important issues that we must always discuss upon. While guardrails must be put on, but there must also be enough leeway, passage for the medium to evolve,” he said.

Mr. Manoharan then took the stage to invite Lt. General Arun Sahni and Mr. Peter Rimmele to give brief remarks.

Lt. General Arun Sahni lauded the development in Meghalaya in recent years. He said, “development activities, connectivity issues have come to be on the positive and are actually making a difference in the state.”

He said that while physical connectivity (road and rail connections) in the state had increased due to efforts of the state and central governments, emotional integration in the Northeast has also grown due to opportunities presented by cyberspace. Now there are more opportunities for people to connect while there is diffusion of ethnic and multi-ethnic conflicts.

However, security remains a concern, said Lt. General Sahni. In particular, fake news propagated through social media has been a problem whose effects trickle down to the law-and-order situation in the region.

Mr. Peter Rimmele who followed Lt. General Sahni alluded to the aspect of peace and prosperity in the Northeast and how cyberspace could threaten it while providing opportunities for growth for the people at the same time. He also invited the Chief Minister to Germany to speak in front of a German audience.

Hon’ble Chief Minister of Meghalaya Mr. Conrad Sangma was then invited to deliver his special address to the audience. He started off by congratulating the organisers for coordinating the event in a physical form in Shillong.

Mr. Sangma said that cyberspace is the most critical subject of our time and that we face a slew of challenges in this domain. He went on to recount his experience starting an Internet Service Provider (ISP) in 1999. While his initial experience was not very successful, he believes it helped spark the evolution of IT in the state. However, there remained still many problems when it came to connectivity in the state.

“We are using technology to the max in governance. I mean I would like to do more but there are limitations on the kind of bandwidth and the kind of connectivity we have in the Northeast which are restrictive. And obviously the manpower and the absorption capacity of the system and the individuals who are working in the large government sectors are huge challenges for us,” he said.

Mr. Sangma elucidated the effect of cyberspace connectivity has had on Meghalaya’s maternal mortality rates.

“We had only 40 per cent mothers actually going for institutional delivery. We started mapping the mothers who were pregnant from villages, to sub-centres, to the doctors who were supposed to take care of them down to the ambulance drivers who are supposed to drive them. So, we went down to micro-details and today thanks to this kind of an e-governance – we call the Mother Programme – we actually were able to increase institutional deliveries to almost double. We’ve touched almost 70 per cent now in a matter of three years,” he said, adding that the mortality rate had come down as a consequence.

E-governance was also being used to monitor roads in the state, he said.

As for the challenges in cyberspace, Mr. Sangma said that cyberattacks are very worrying. “So, this information is great for governance, but it opens up another challenge for us where we are actually exposing the entire details of all the patients or all the pregnant mothers we have in our state,” he said, stressing that his government was working to ensure safe and secure Virtual Private Networks were used in most cases to minimise access.

Next, Mr. Sangma also touched upon the law-and-order situation in the Northeast vis-à-vis cyberspace connectivity. When a threat arises, the immediate response of government officials is to cut mobile connectivity and internet services. This is even before the police get involved, said Mr. Sangma. While these measures are taken to curtail the chance of mobilisation and diffusion of fake news, government authorities are concerned about obstacles caused to individuals.

“We are as a government looking at ways and means in which we can actually start going into stopping specific services without disrupting the range of services that are there. How do we segregate the areas that are necessary services through the Internet and blocking the ones which will actually cause the problem is a true issue and problem for the government?” he said.

Mr. Sangma then spoke about other instances where the cyberspace impacted governance in India. Defence, he pressed, was a concern and the Government of India has from time to time advised not to use products by certain actors – both state and non-state – it considers dubious lest they fall to hackers.

“We need to work towards some kind of laws and policies that could actually balance this out and be acceptable. I know it’s a very easy thing to say, but it is very difficult. Nations are struggling to find out where that particular balance will come in,” said Mr. Sangma, adding that the entire dynamics of warfare is changing.

Alluding to economic development of the Northeast, Mr. Sangma said that the reason for the unrest in the region as a whole has been a lack of development and socio-economic factors. “Socio-economic aspects of development need to go hand-in-hand while we come out with policies for peace,” he said.

To conclude his address, Mr. Sangma said that the youth in the Northeast was highly engaged and enterprising thanks to cyberspace but the challenge remains in converting their passions into livelihood. He said that he felt strongly about harnessing the talent and enterprise of the youth to alleviate the region economically, though there might exist many challenges. Mr. Sangma said that he would reflect upon the outcome of the conference and take the knowledge gained to national level discussions on cyberspace.

Next in the programme was **Session VI: Cyberspace and neighbourhood threats.**

It was chaired by Ambassador Ruchi Ghanashyam IFS (Retd). She highlighted the transcendence of cyberspace across physical boundaries, recalling the example of STUXNET malware attack which was talked about during this conference.

“It is the neighbours that have issues which are most likely to be complex and the intent that may exist between the two may not necessarily be there for others [in immediate neighbourhood or far away],” she said, stressing that cyber threats in the neighbourhood were a matter of politics and international relations.

“For India, I think all issues are of concern, whether it is security issues or whether it is privacy or whether it is businesses – from every aspect I think cyberspace is important,” she continued.

Amb. Ghanashyam then introduced the physical and virtual speakers in the session.

The first speaker joined in virtually from Israel. Lt. Colonel Ofer Rotberg (Retd), Head of Cyber Security, Elbit Systems leads the CyberShield programme to protect weapons systems, C2 networks and future battlefield. He stressed the importance of civilian and military dependency.

“If you look at the cybersecurity perspective, and you want to defend your critical assets, this should cover also services that are less critical but are part of the chain,” he said.

He explained the connection between cyberspace and other four traditional domains of air, land, maritime and space, saying that they were all integrated. When considering future battlefields every military should consider all domains together, he said.

“The cyberspace domain is the future battlefield and will be tightly connected to the other domains and these will be multi-domain operations,” he said, adding that, for example, anti-missile equipment and even submarine GPS systems could be easily jammed by cyber tools.

Lt. Col. Rotberg spoke of cyber protection for weapon systems, saying that main weapons systems of many countries are not as secure as they should be against evolving threats.

He ended his address by giving suggestions on how policy and decision makers can go forward with securing cyberspace.

“Recent events are a wake-up call for decision makers to start promoting a program to protect critical assets, focussing on military critical assets but it can be broadened. We should assess the risks, take into consideration the exposure level of critical systems and the potential impact. We should start of course from the systems that are the most critical. The programme should not only cover the tools but we should also consider the people that are going to run those tools and we should also talk about the processes,” he said.

The next speaker was Dr. Adam Svendsen, an intelligence and defence strategist, associate consultant at the Copenhagen Institute for Futures Studies, Denmark. Joining the summit virtually, he based his speech on Cyber Intelligence (CYBINT).

“Cyber intelligence is acquiring, processing, analysing and disseminating information that identifies, tracks and predicts, threats, risks and opportunities in the cyber domain to offer courses of action that enhance decision making,” he explained, quoting a US report.

The speaker examined the structure of CYBINT work to conduct of CYBINT, with a strong System-of-Systems (SoS) approach. CYBINT work can be broken down into a combination of human and machine teaming in the context of the environment, in this case the neighbourhood, elucidated Dr. Svendsen.

Dr. Svendsen argued that when thinking in terms of course(s) of action (CoA), CYBINT work could be evaluated as consisting of and ranging from ‘Wait & Watch’ (intelligence methodology) postures to more ‘See & Strike’ (military/security/law-enforcement methodology) approaches.

He gave an overview of the insights involved when evaluating threats in the neighbourhood. One must consider the key actors involved, forces and factors of change (concerning what activity) and possible changes overtime (when and where the events might be occurring), he explained.

Dr. Svendsen summed up by saying, “The whole is more than the individual sum of parts when dealing with cyber intelligence enterprises and the SoS-engineering-based approach. Situational awareness is key”.

The final speaker for this session was Dr. Gudrun Wacker, Chinese foreign and security policy expert at the Stiftung Wissenschaft und Politik (SWP), Berlin, Germany. She conceptualised cyberspace as an element in the toolbox of China’s geopolitical strategy. In particular, she spoke of China’s grey zone and cyber activities vis-à-vis Taiwan.

Cyberspace falls under the category of unrestricted warfare for China, an ideology developed in the late 1990s, she said. “The main attributes of this are its hybridity – you can also call that multi-domain. It goes beyond the military sphere, its irregular warfare, its non-contact, non-linear and its non-symmetric,” she said, adding that one could hardly even identify a real battlefield now.

“The threats are always lingering and there are no clear demarcation lines between military, political, economic and social means and between state, state-sponsored non-state actors,” said Dr. Wacker.

Over the last two decades, China has developed a carrot-and-stick toolbox but lately it has been employing the stick more than the carrot, she said. Dr. Wacker pointed to the astonishing number of Chinese cyber-attacks per day, going into the millions. An example was the November 10, 2021 report by the Taiwanese Director for Cybersecurity that Taiwan was subject to five million cyber-attacks and scans every day. These scans and attacks have been trying to find vulnerabilities in the systems and about 50 per cent of these attacks are believed to originate from China.

Dr. Wacker also mentioned the targeted disinformation in social media, economic cohesion by stopping Chinese tourists from going to Taiwan, the boycotting of pineapples, incursions by PLA Air Force, military activities in the South China sea and soft multigenerational tools to make future generations more pliant.

To conclude, Dr. Wacker reverted to the “carrot-and-stick” idea of China’s toolbox. “So, the carrots are still there to show what would happen if Taiwan would finally give up this ‘stupid’ idea of being a separate entity,” she said. The tools are too small for bigger powers like the US to intervene.

The ultimate purpose of these efforts, she said was to undermine the trust in the government by spreading misinformation (a way is visual aids), intimidate the people (by showing military power), wear down and demoralise the Taiwanese and create a sense of defeatism where the people would want to throw in the towel and accept Chinese supremacy.

Valedictory Session

The valedictory address “Cyberspace War: Defending and Protecting India” was delivered by Mr. Navin Kumar Singh, IPS, Director General National Critical Information Infrastructure Protection Centre (NCIIPC).

“Security experts often observe that the next war will be fought not on land, sea, air, water or underwater but in the virtual cyberspace. This is because of the increase dependence on cyberspace for almost everything,” said Mr. Singh, adding that perpetrators were not geographically bound and conventional wars without a cyber element are very unlikely.

“Cybersecurity is going to be the lifeline of national security,” he stressed. He noted Chinese Premiere Xi Jinping’s 2014 remarks on how Internet security and informatisation are major issues concerning the security, economy and overall development of a country.

Mr. Singh went on to elaborate on seven critical sectors in India that need protection including banking and finance, health, power and energy, strategic and public enterprise, transport, government and defence. Cyber threats were also aimed at India's Research and Development (R&D) and Intellectual Property Rights (IPR) spheres, he said adding that a particular company could be targeted to promote its rivals.

Of the role of the NCIIPC, Mr. Singh said, "One of our most important activities is the active threat monitoring in the Indian cyberspace and this is what we are doing through our national cyber analytic centre." An important source of information for the NCIIPC is NetFlow monitoring software.

Next, Mr. Singh also spoke of the importance of the private sector in the Indian cyberspace, a thought that was mirrored by many speakers during the two-day conference. Private players were everywhere – from banking to power, energy to transport.

"In this age of liberalisation, many of the important Critical Information Infrastructures (CIIs) are in the private sector only. This needs to be kept in mind when we are talking about defending India in the cyberspace wars," he said.

Mr. Singh also advised that a proactive risk-based approach to improving cybersecurity was needed, along with mitigation strategies, crime laws and acts to deal with cyber-attacks .

"If mitigation is not possible, we should be aware of the residual risks which we are living with. We need to enforce the minimum cybersecurity standards and framework," he said.

Continuous threat-hunting, evaluation and monitoring of adversaries, adaption to newer technology, managing supply-chain infrastructure was to be kept in mind, he said, when dealing with the Indian cyberspace. Like other speakers, Mr. Singh concluded by reiterating that the strategy of offense being the best form of defense in the cyberspace.

To conclude the conference, Mr. Pankaj Madan, Deputy Head, India Office of the Konrad-Adenauer-Stiftung, summed up all the participants' contributions over the two days. His address was followed by a vote of thanks by Ms. Nisha Ramdas, Conference Director, Director, Global Dialogue Forum.

PREAMBLE

A future world dominated by cyberspace is being shaped before our eyes. It has already influenced and redefined many vital concerns of humankind — from defence and security to the environment to health to social life.

Its algorithms will in time accurately predict what is to come; based on data from the past and present, to hopefully enhance the quality of life.

It is indeed a 'Fifth Frontier' — laying down the contours and content of a world order that was previously determined by dominance of land, water, air and space. Analysing this 'Fifth Frontier' — with its threats and opportunities — will form the substance of this conference.

On this frontier will wars be fought and peace won, using technological advancements to build equitable economic prosperity and environmental sustainability.

In fact, the potential for good and evil is a challenge and opportunity confronting humanity, as its leaders and influencers come to terms with cyberspace.

The distancing of human, physical engagement in war-fighting and in penetrating personal privacies will probably deepen the divide between the developed and developing world, even as they raise grave concerns over widely cherished principles of privacy.

That these advancements over cyberspace will emphatically impact and alter human behaviour seems certain.

It could also result in a new and frightening Cold War, spearheaded by both old and new antagonists.

The Cyber conflicts — already raging in low intensity — have the potential to flare into horrific wars that cause suffering on a far greater scale than conventional weapons when critical infrastructure is penetrated.

The threat of nuclear war may even be overshadowed by potential attacks on critical national infrastructure, from energy to telecom to health, with equally, if not greater devastating consequences.

Cyber-defensive and cyber-offensive abilities will come to define the great military powers.

Cyberspace's accessibility has indeed opened the floodgates to the involvement of state and non-state actors, including corporates and individuals.

Both hacktivist and terrorist will find voice in this space.

This has thrown up dilemmas that include bridging the gulf between cyberspace's open and secure forms, traditional notions of sovereignty in evolving global rules of engagement, digital democracy and diplomacy, protecting data, enforcing legal protocols and upholding ethical values.

Amidst the globalisation of information, cyberspace itself faces several technological challenges, ranging from innovations in theory and in application.

This conference will discuss the possible transition from the traditional to a new global cyberspace, whose characteristics are openness, heterogeneity, mobility, dynamism, and security.

The realisation is dawning that of cyberspace security is a high priority.

Compared with traditional network security, future cyberspace security will have to consider the obsolescence of traditional static methods based on known threat characteristics in order to effectively defend against novel forms.

**GLOBAL DIALOGUE FORUM
&
THE INDIA OFFICE OF THE KONRAD ADENAUER STIFTUNG**

Present

The Global Dialogue Security Summit 2021

Managing Cyberspace in the Indo Pacific

Date: Wednesday/Thursday, November 24-25, 2021

Mode – Hybrid

DAY I

1000 hrs – 1100 hrs: INAUGURAL SESSION

Introductory Remarks: Mr. Moses Manoharan, Chairman, Global Dialogue Forum

An Indian Perspective: Ambassador Ruchi Ghanashyam IFS (Retd), India's former High Commissioner to the UK, Chairperson Conference Organising Committee

A European Perspective: Mr. Peter Max Rimmele, Resident Representative to India, Konrad Adenauer Stiftung

Keynote Address: Lt General (Dr) Rajesh Pant, PVSM, AVSM, VSM (Retd), National Cyber Security Coordinator

Presenter: Ms. Abha Myllemngap

Coffee Break: 1100 hrs – 1130 hrs

1145 hrs – 1315 hrs SESSION I: DEFINING CYBERSPACE AND IDENTIFYING ITS CHALLENGES

Chair: Major General Lav Bikram Chand, VSM, (Retd), Corps of Signals, Indian Armed Forces

Speaker: Vice Admiral Professor Dr. Ir. Amarulla Octavian, S.T., M.Sc., DESD., of the Indonesian Navy, is Rector of the Republic of Indonesia Defense University

Speaker: Mr. Md. Nobir Uddin, Senior System Analyst, ICT Division, Ministry of Posts, Telecommunications and Information Technology, Government of Bangladesh

Speaker: Brigadier Ashish Chhibbar, Senior Fellow with the Strategic Technologies Centre at the Manohar Parrikar Institute for Defence Studies and Analyses in New Delhi, Specialist in Artificial Intelligence

Lunch: 1330 hrs – 1430 hrs

1445 hrs – 1640 hrs SESSION II: COLLABORATION AND CONFLICT OVER CYBERSPACE IN THE INDO PACIFIC

Chair: Lt. General Arun Kumar Sahni, PVSM UYSM, SM, VSM (Retd), Former General Officer Commanding in Chief, South Western Command involved in armed forces cyber, digitisation and network enablement

Speaker: Mr. Amit Sharma, Advisor (Cyber), Defence and Research Development Organisation (DRDO)/Office of the Secretary Department of Defence(R&D), Ministry of Defence, Government of India

Speaker: Dr. Geoff Heriot, Member of Council (Management Committee), Tasmanian branch of the Australian Institute of International Affairs, one of Australia's oldest think tanks (virtual mode)

Speaker: Mr. Alok Sinha, Chief Executive Officer, Globus Eight Inc., Gurgaon (virtual mode)

HIGH TEA: 1640 hrs – 1715 hrs

1715 hrs – 1830 hrs SESSION III: Cyberspace in Industrial Development

Chair: Ambassador AR Ghanashyam IFS (Retd), India's former envoy to Nigeria, alumnus of Indian Institute of Management, Ahmedabad

Speaker: Prof. Dr. Heribert Dieter, Economist, Stiftung Wissenschaft und Politik, Berlin, Germany

Speaker: Mr. Ravi Nirgudkar, Managing Director, BAE Systems, India

Speaker: Mr. Argha Bose, Head Cyber Security, Tata Advance Systems Ltd.

DINNER RECEPTION: 1930 hrs – 2200 hrs

DAY II

1000 hrs – 1130 hrs SESSION IV: CONVENTIONAL WAR, CYBERSPACE AND SOVEREIGNTY

Chair: Lieutenant General Sunil Srivastava, AVSM, VSM** (Retd), Director, Centre for Joint Warfare Studies (CENJOWS)

Speaker: Mr. K.P.M. Das, National Cyber Security, Cisco (virtual mode)

Speaker: Mr. George Mikaberidze, CEO, JSC Rosinfocominvest, Moscow, Russia (virtual mode)

Speaker: Mr. Shreyas Jayasimha, specialist in cyber and space laws, Founding partner Aarna Law

COFFEE BREAK 1130 hrs – 1200 hrs

1200 hrs – 1130 hrs SESSION V: CYBERSPACE CONNECTIVITY FOR PEACE AND DEVELOPMENT IN INDIA'S NORTHEAST

With a special address by Hon'ble Chief Minister of Meghalaya, Mr. Conrad Sangma

Chair: Hon'ble Member of Parliament Mr. K.J. Alphons, Member, Parliamentary Standing Committee on External Affairs is a former senior Indian civil servant and advocate from Kerala. He is India's former Minister of State for Culture, and Tourism

Speaker: Dr. Pfokrelo Kapesa, Assistant Professor, International Relations, Northeast Christian University (NECU), Dimapur, Nagaland

Speaker: Hon'ble Member of the State Assembly of Arunachal Pradesh, Mutchu Mithi

LUNCH: 1400 hrs – 1500

1515 hrs – 1730 hrs SESSION VI: CYBERSPACE AND NEIGHBOURHOOD THREATS

Chair: Ambassador Ruchi Ghanashyam IFS (Retd), India's former High Commissioner to the UK, Chairperson Conference Organising Committee

Speaker: Lt. Col. Ofer Rotberg (Retd), Head of Cyber-Security, Elbit Systems, where he leads the CyberShield programme to protect weapons systems, C2 networks and future battlefield (virtual mode)

Speaker: Dr. Adam D.M. Svendsen, an intelligence and defence strategist, associate consultant at the Copenhagen Institute for Future Studies, Denmark (virtual mode)

Speaker: Dr. Gudrun Wacker, Senior Fellow in the Asia Division at the German Institute for International and Security Affairs (Stiftung Wissenschaft und Politik, SWP)

VALEDICTORY ADDRESS 1745 hrs – 1830 hrs

Cyberspace War - Protecting and Defending India

Speaker: Mr. Navin Kumar Singh IPS, Director General, National Critical Information Infrastructure Protection Centre (NCIIPC)

Summing up: Mr. Pankaj Madan, Deputy Head, Konrad Adenauer Stiftung, Delhi, India

Vote of Thanks: Ms. Nisha Ramdas, Conference Director, Director, Global Dialogue Forum

DINNER RECEPTION: 1900 hrs ONWARDS

SUMMIT CONCLUDES

CURRICULUM VITAE

Hon'ble Chief Minister of Meghalaya state, Mr. Conrad Sangma, is also president of the National People's Party, succeeding his late father and former Chief Minister of Meghalaya, Mr. P. A. Sangma. Mr. Conrad Sangma was Member of Parliament from Tura and the youngest Finance Minister of Meghalaya. He has previously held several important portfolios in the state cabinet, including Finance, Power, Tourism, and IT. Apart from politics, Mr. Sangma is president of the PA Sangma Foundation for the betterment of education and environment, and he also runs four colleges in rural Meghalaya. He also currently serves as President of the Meghalaya Cricket Association and Sports Academy.

Ambassador Ruchi Ghanashyam IFS (Retd), a distinguished Indian Diplomat, has been High Commissioner of India to the UK and Envoy to the Commonwealth in a career spanning 38 years. She had also served in Indian Diplomatic Missions in Damascus, Kathmandu, Brussels, Islamabad and as part of India's Permanent Mission to the UN. She has been High Commissioner to both Ghana and South Africa.

Mr. Peter Max Rimmele is currently the Resident Representative of Konrad-Adenauer-Stiftung Office, India. He has a First Law Degree from Freiburg University, as well as a Second Law Degree from the Ministry of Justice Baden Württemberg, Germany and a M.A. in Geography. After working as a jurist, judge and lecturer, he took public office as Ministerialrat, Head of Division at the State Ministry of the Interior in Saxony, Germany, from November 1991 on until 2000. There he first served in the Police and Security and later in the Local Government Department. On behalf of the German Foreign Ministry he served in East Timor as Registrar General, Head of Civil Registry and Notary Services (UNTAET), and became later the principal Advisor for Governance Reform for GIZ (German International Cooperation) to the Ministry of Administrative Reform and the Anti-Corruption-Commission of the Republic of Indonesia, where he served for 7 years. He then moved to Rwanda, also as Principal Advisor Good Governance/Justice Program. Earlier he was Resident Representative Lebanon, Director of Rule of Law Program Middle East North Africa, Konrad-Adenauer-Stiftung.

Lt General (Dr) Rajesh Pant, PVSM, AVSM, VSM (Retd) an internationally recognised Cyber Security expert, holds the prestigious position of National Cyber Security Coordinator. In this capacity he oversees all activities across multiple sectors to ensure a secure and resilient cyber space within India. A PhD in Information Security metrics, he has headed the Army's Cyber Training establishment in the Signals Corps for 41 years, and thrice awarded for distinguished service of the highest order by the President of India for distinguished service of the highest order.

Major General Lav Bikram Chand, VSM, (Retd): during his 37 years of active service in Corps of Signals, he gained expertise in Software Development for Integrated Electronic Systems & Communications for Tac C3I systems, managing main frame computer centres, roll out of Pan India Army Static Switched Network (ASCON) and its associated Network Operating Centres,

Security Operating Centres and Data Centres. At Headquarters, Integrated Defence Staff, he was responsible for Spectrum Management, Joint EW and EMI/EMC as well as Coordinating the Network For Spectrum's Design and Implementation Document. As Additional Director General, Telecommunications he also oversaw Network Security of Army Data Networks. He holds an Masters from IIT Madras, Masters in Management Studies from Osmania University and in Artificial Intelligence from Austin University. Post retirement he has focused on High Capacity Software Defined Radios MANET (Mobile Adhoc Network) and 5G.

Vice Admiral Professor Dr. Ir. Amarulla Octavian, S.T., M.Sc., DESD., Of the Indonesian Navy, is Rector of the Republic of Indonesia Defense University. He has attended the Royal Australian Navy Maritime Studies and Good Governance and Conflict Training Course in Den Haag. After Naval Command and Staff College and Collège Interarmées de Défense in France, he completed courses in Combined Force Maritime Component Commander Flag Officer Course and Transnational Security Cooperation Course in Hawaii, US. He has been Commander, Sangatta Naval Base and ADC to the President of Indonesia. He was then elevated to Commander, Sea Battle Group, Western Fleet Command, Chief of Staff, Western Fleet Command, and Commander, Naval Staff and Command College. He holds a Master of Science degree from Université Paris 2 Panthéon-Assas and a doctorate on military sociology from University of Indonesia. He has been a visiting professor to the Japan National Defense Academy, and the PLA National Defense University. He has been awarded 8 stars and 13 medals of honor.

Mr. Md. Nobir Uddin, Senior System Analyst, ICT Division, Ministry of Posts, Telecommunications and Information Technology, Government of Bangladesh, is a Certified Security Analyst (CSA), with a Masters degree in Computer Science and Engineering, and a Diploma in E-Governance and informatics, South Korea.

Brigadier Ashish Chhibbar, Senior Fellow with the Strategic Technologies Centre at the Manohar Parrikar Institute for Defence Studies and Analyses in New Delhi, his areas of focus are cyberspace policy and disruptive technologies of Artificial Intelligence, block chain and big data analysis. Brigadier Chhibbar is an alumnus of the Military College of Telecommunication Engineering, and varied operational experience.

Lt. General Arun Kumar Sahni, PVSM UYSM, SM, VSM (Retd), Former General Officer Commanding in Chief, South Western Command, and Director General, Indian National Association, Club of Rome, is a highly decorated, scholar-soldier, with 40 years of commissioned service in the Indian Army. He is a recipient of the Seva Medal (SM) & Vishisht Seva Medal (VSM) while in service in operational areas, the Uttam Yudh Seva Medal (UYSM) for command of the operational Corps in the Northeast and the Param Vishisht Seva Medal (PVSM) for his meritorious service in the army. Additionally, he has been awarded the Chief

of Army Staff Commendation Card twice. He is a Distinguished Fellow with two premier think tanks in Delhi and an advisor to a major corporate in its defence initiatives. He is an avid golfer and polo player and was the Vice President of Indian Polo Association. He has served in different operational environments of Sri Lanka, North East, and trained with the British Army, was a military diplomat in Russia. In Military Operations, he dealt with structuring and capability development and Information Technology.

Presently 'pro bono', he is mentoring start-ups in the domain of cyber, robotics and AI. A trustee of an environmental policy group that he actively steers and he is on the managing board of a well reputed public school and University. He is a Distinguished Fellow with two premier think tanks in Delhi and an advisor to a major corporate in its defence initiatives. He is an avid golfer and polo player and was the Vice President of Indian Polo Association.

Amit Sharma is Advisor(Cyber) and Director in the Office of the Secretary Department of Defence(R&D). He also represents India in the United Nations Governmental Group of Experts, UN GGE and United Nations Open-Ended Working Group UN OEWG for Cyber related issues as member of Indian delegation. He is a Chevening Scholar and has gained his Masters in 'Global Security' from the Defence College of Management and Technology, UK Defence Academy, United Kingdom and is a graduate/fellow of the DoD's Asia Pacific Centre for Security Studies, in Hawaii US. He has also been a member of various committees and taskforces in consultations with various countries, including for the Indo US homeland security bilateral. He was invited to the NATO Centre of Excellence on Cyber Defence as an international expert to review the Tallinn Manual 2.0.

Geoff Heriot, Member of the Council of the Tasmanian branch of the Australian Institute of International Affairs, one of Australia's oldest think tanks, is a former foreign correspondent and executive with the Australian Broadcasting Corporation (ABC), widely travelled in South Asia and the Pacific, and a consultant on media and governance. His senior ABC appointments included Chief of Corporate Planning and Governance, General Manager of Corporate Strategy, and Controller of News and Programmes at the multilingual international service, Radio Australia. He was seconded as adviser to the post-Apartheid board chairperson and the chief executive of the South African Broadcasting Corporation from 1994-96.

Mr. Alok Sinha Alok Sinha, CEO, Globus Eight: An alumnus of Harvard Business School, Mr. Sinha is the founder and CEO of Globus Eight group of companies located in New York, Dubai, and Gurgaon, India, in Cyber Security and AI. He has managed the IBM Global Grid computing, Tata teleservices and Huawei Enterprise business. He was Chief of Information Security for the Bharti (Airtel) group's largest IoT framework.

Ambassador AR Ghanashyam, IFS (Retd) is a distinguished Indian diplomat who served as India's Ambassador to Angola and High Commissioner to Nigeria. An alumnus of the Indian Institute of Management Ahmedabad, he is an adviser and a commentator on foreign policy and energy issues.

Prof. Dr. Heribert Dieter is Senior Fellow at the German Institute for International and Security Affairs, Visiting Professor of International Political Economy, Zeppelin University, Lake Constance (since 2013) and Adjunct Professor at the University of Potsdam (since 2017). He studied Political Science and Economics at the Free University of Berlin. After his position as a Senior Fellow at the University of Duisburg researching global economy and regional integration he joined the Central European University, Budapest as a visiting Professor in 2004. From 2005 to 2010 he worked as a Coordinator, a Member and Principal Writer of the „Warwick Commission on the Future of the Multilateral Trading System “and a Member and Co-Director of the “Warwick Commission on International Financial Reform” at the University of Warwick. During that time, he also was a visiting Researcher and Professor at the University of Sydney and submitted his habilitation in political science. Besides his current positions he has been Professor and Chair of International Relations at Ruhr University Bochum and Visiting Professor at the Australian National University, Canberra; Murdoch University, Perth. His current research focused on the future of globalization, the consequences of rise of China for the world, Bilateralism and plurilateralism in trade governance and Germany's position in the 21st century's global economy.

Mr. Ravi Nirgudkar is Managing Director for BAE Systems in India, Bangladesh, and Sri Lanka. BAE Systems is a technology and innovation leader specializing in defense, aerospace and security solutions. Mr. Nirgudkar has 27 years service in international business development and programme management in defense, space, aerospace and international markets. He was previously Raytheon's Country President for India, Bangladesh, and Sri Lanka. He has served as Programme Director on Protected Satellite Communications Systems responsible for strategy development and evaluation of new growth areas. Earlier, as International Business Executive, he was responsible for strategic growth and public policy in India, UAE, KSA, Australia, UK, and Canada in the areas of Satellite Communications, Unmanned Systems, Environmental Solutions, and ISR Systems.

Mr. Argha Bose, Head, Cyber Security, at Tata Advanced System Ltd., is focused on Cyber Security, in which he has more than two decades experience in Consulting, Practice and Delivery Management, Pre-sales, Business Development, addressing Indian and global customers. He leads his organisation's capabilities towards the achievement of long and short terms goals while managing diversified teams.

Lieutenant General Sunil Srivastava, AVSM, VSM (Retd)**, Director, Centre for Joint Warfare Studies (CENJOWS) has commanded a Field Artillery Regiment and an Infantry Brigade on the Line of Control in Jammu and Kashmir, and an Infantry Division on the Line of Actual Control in the Northeast. As a Lieutenant General, he served as Chief of Staff, Eastern Command. He also served as Senior Faculty for over two years at the National Defence College, New Delhi. He was the Commandant, Officers Training Academy at Gaya.

Mr. K.P.M. Das is the National Cybersecurity and Trust Officer for Cisco, driving emerging cyber security initiatives in India and Asia Pacific. Previously, he with the Indian Army for 25 years. He had a one year stint with the UN in Angola as a Military Observer, overseeing post-elections political processes in 1994. He ran the Information/Cyber Warfare Cell in the Military Operations Directorate at Army HQ during the Kargil War, and commanded an Infantry Division Signal Regiment during Operation Parakram in 2002. KPM has also been an Instructor at Military College of Telecommunication Engineering, teaching data structures, algorithms and systems programming.

Mr. George Mikaberidze, CEO, JSC Rosinfocominvest, a state-owned agency responsible for Russian IT export. He has more than 20 years of experience in M&A, new business development and market expansion. He was co-founder and CEO of 100AM Corporation, which develops business networking platforms. He has been Vice President for Business Development and Marketing, RBC Media Holding – a leading Russian Business Media Holding which owns TV channel, news portals and other media.

Mr. Shreyas Jayasimha, Head of Aarna Law, Aarna ADR, Singapore, is a space, technology and nuclear law specialist. He is an Advocate, Arbitrator and Mediator with more than two decades of experience in complex domestic and international dispute resolution. His practice areas include international commercial and investment law, space law, technology and nuclear law.

Hon'ble Member of Parliament Mr. K.J. Alphons, Member, Parliamentary Standing Committee on External Affairs is a former senior Indian civil servant and advocate from Kerala. He is India's former Minister of State for Culture, and Tourism. He is currently serving as a Member of Parliament, In the Rajya Sabha from the state of Rajasthan. Alphons. He was in the Indian Administrative Service, Kerala cadre. He has served as Commissioner of the Delhi Development Authority and a Member of the Legislative Assembly from Kerala.

Dr Kapesa Pfokrelo teaches International Relations at North East Christian University, Dimapur (Nagaland). She has a PhD in Diplomacy and Disarmament from Jawaharlal Nehru University. Her research interest includes Peace and Conflict Studies, Security Studies,

Geopolitics, Neocolonialism, Indigenous Peoples' Worldview and Diplomacy and Gender Studies.

Hon'ble Member of the State Assembly of Arunachal Pradesh, Mutchu Mithi, is a young generation leader from India's Northeast. He was elected from Roing seat to the Arunachal Pradesh Legislative Assembly. Situated in the Lower Dibang Valley, it is on the north-eastern frontier of India.

Lt. Col. Ofer Rotberg (Retd) is a veteran in the field of cyber security, with more than 25 years of experience in research, development, strategic planning and operations. Prior to joining Elbit, Mr. Ofer held senior positions in elite IDF cyber units. Today, Ofer leads the CyberShield program with the goal of protecting weapons systems, C2 networks and the future battlefield.

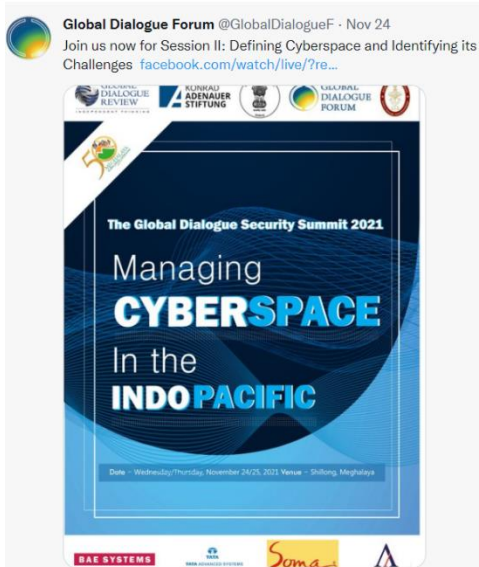
Dr. Adam D.M. Svendsen is an established international intelligence and defence strategist, educator, researcher, analyst, and consultant. He has multi-sector experience and co-runs the Bridgehead Institute (Research & Consulting - Insight, Training & Education), is an Affiliated Scientist and Visiting Guest at the Collective Intelligence Group at the IT University of Copenhagen (ITU), as well as an Associate Consultant at the Copenhagen Institute for Futures Studies (CIFS), Denmark. He also lectures & advises from design to implementation as an 'academic director' on 'Global Security & Intelligence' for the Global & International Studies Masters Programme courses at the University of Salamanca, Spain. He has been a Visiting Scholar at the Center for Peace and Security Studies (CPASS - now, the Center for Security Studies (CSS)), Georgetown University, and held a post-doctoral fellowship based in the Centre for Military Studies (CMS), Department of Political Science, University of Copenhagen, Denmark, and he has worked on the International Security Programme at Chatham House (the British Royal Institute of International Affairs) and at the International Institute for Strategic Studies (IISS), London.

Dr. Gudrun Wacker is at present Senior Fellow in the Asia Division at the German Institute for International and Security Affairs (Stiftung Wissenschaft und Politik, SWP) in Berlin, a think tank providing political advice to the German government and parliament. Her research focuses on Chinese foreign and security policy, especially EU-China relations, China and the Asia-Pacific region, security cooperation in the Asia-Pacific and the Indo-Pacific. She is currently an EU delegate to the Experts and Eminent Persons Group of the ASEAN Regional Forum.

Mr. Navin Kumar Singh IPS, Director General, National Critical Information Infrastructure Protection Centre, is a senior, reputed police official. His institution is the nodal agency protecting India's information structure from threats ranging from cyber terrorism to cyber warfare.

Mr. Pankaj Madan is Advisor and Team Leader - Programmes at the New Delhi Office of the Konrad Adenauer Foundation. He has been with the Foundation for 22 years in various capacities; and is responsible for conceptualization of development and dialogue programmes, research and editing, budgetary evaluations and monitoring and liaising with Ministries at state and centre levels, Members of Parliament and State Legislatures, Government Departments, Political Parties, Media and Apex bodies. Previously, he was with Indo-German Export Promotion (IGEP) project of the GIZ.

SOCIAL MEDIA







Global Dialogue Forum @GlobalDialogueF · Nov 24
Md. Nobir Uddin, Govt of Bangladesh at the #GDSS2021
#CybersecuritySummit @KASonline @KASMediaAsia



1



Global Dialogue Forum @GlobalDialogueF · Nov 24
Prof. Dr. Heribert Dieter at the #GDSS2021 #Cybersecurity #cyberspace
@SWP_Global @KASonline



1



Global Dialogue Forum
@GlobalDialogueF

Join us now for #GDSS2021 Session III: Collaboration and conflict over cyberspace in the Indo Pacific chaired by Lt Gen Arun Sahni (Retd)
@KASonline
@KASMediaAsia facebook.com/globaldialogue...



2:41 PM · Nov 24, 2021 · Twitter Web App



Global Dialogue Forum @GlobalDialogueF · Nov 24
Replying to @GlobalDialogueF

China's impact should be taken into account when we talk about cyberspace, says Lt. Gen Sahni. #GDSS2021 @KASonline #Cyberspace #IndoPacific

1



Global Dialogue Forum @GlobalDialogueF · Nov 24

Collaborative efforts have been emerging in the cyberspace incl. at ASEAN and ASEAN Regional Forum to combat cybersecurity threats, says Lt. Gen. Sahni #GDSS2021 @KASonline @KASonline #Cyberspace #IndoPacific

1



Global Dialogue Forum @GlobalDialogueF · Nov 24

Cyberspace was a blind spot of the South Asian region but now BRICS and BIMSTEC are addressing this particular area and its challenges, says Lt. Gen. Arun Sahni #GDSS2021 #Cyberspace #IndoPacific @KASonline @KASMediaAsia

1



Global Dialogue Forum
@GlobalDialogueF

Brig Ashish Chibbar at the #GDSS2021, author of the book "Navigating the Indian Cyberspace Maze: Guide for Policymakers" @KASonline



Manohar Parrikar IDSA, New Delhi

12:53 PM · Nov 24, 2021 · Twitter Web App



Global Dialogue Forum @GlobalDialogueF · Nov 24
Replying to @GlobalDialogueF

India has highest AI skill penetration rate in the world
AI specialist is the second emerging job role in India in 2020 and has deep economic benefits. Many tech startups in India are based on AI tech: Brig Ashish Chibbar at #GDSS2021 @KASonline @EU_in_India @IDSAIndia

1



Global Dialogue Forum @GlobalDialogueF · Nov 24

Brig Chibbar: India generates the world's largest data per month. We need to reward R&D by making it a lucrative vocation. #GDSS2021 @KASonline @EU_in_India @IDSAIndia

1



Add another Tweet



Global Dialogue Forum @GlobalDialogueF · Nov 24
Replying to @GlobalDialogueF

Brig Ashish Chibbar: We can use AI to improve governance systems, digital delivery of services and also provide world with clean affordable and good systems to be shared worldwide. #GDSS2021 @KASonline #cybersecurity

1



Global Dialogue Forum @GlobalDialogueF · Nov 24

.@GudrunWacker at the #GDSS2021 @SWPBerlin @SWP_Global @KASonline @EU_in_India



1

Global Dialogue Forum @GlobalDialogueF · Nov 24

Amit Sharma, Cyber Advisor, DRDO: Three main realms of cyberspace that exchange hands quite often are cyber crime, cyber terrorism and cyber warfare. Most sensitive of the three is cyber warfare #GDSS2021 @KASonline @KASMediaAsia #cyberspace

Global Dialogue Forum @GlobalDialogueF · Nov 24

Amit Sharma: we can only achieve a strong cyber defence system if we have global and collaborative leadership in technology #GDSS2021 @KASonline #Cyberspace #IndoPacific

Global Dialogue Forum @GlobalDialogueF · Nov 24

Join us for Session III Cyberspace in Industrial Development #GDSS2021 @KASonline #Cyberspace #indopacific facebook.com/globaldialogue...



Global Dialogue Forum @GlobalDialogueF

.@CENJOWS Director Lt Gen Sunil Srivastava at the #GDSS2021 @KASonline @CMO_Meghalaya #indopacific #cyberspace

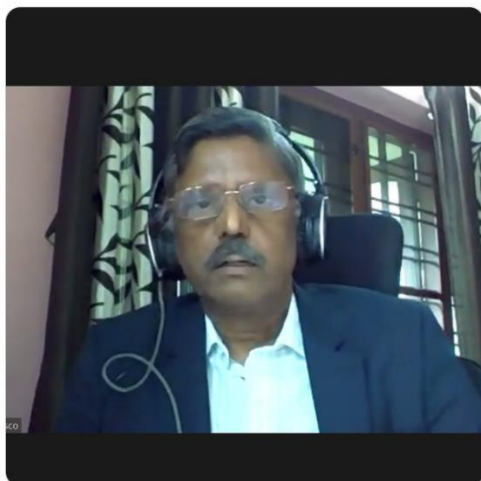
Translate Tweet



10:32 AM · Nov 25, 2021 · TweetDeck

Global Dialogue Forum @GlobalDialogueF · Nov 25

.@cisco_in KPM Das at the #GDSS2021 @KASonline @CENJOWS #IndoPacific #cyberspace



Global Dialogue Forum @GlobalDialogueF · Nov 25

.@CMO_Meghalaya Hon'ble Chief Minister of Meghalaya @SangmaConrad will join us today at the #GDSS2021 Tune in: @CENJOWS @KASonline #IndoPacific #Cyberspace bit.ly/3HNGzVr



Global Dialogue Forum @GlobalDialogueF · Nov 25

Replying to @GlobalDialogueF

.@CENJOWS Director, Lt. Gen Srivastava: Its no more a situation of binary relationship of war or peace with states. There are both state and non state actors involved. Violence is predominant means of coercion. War strategies have become hybrid. #GDSS2021 #cyberspace @KASonline

Global Dialogue Forum @GlobalDialogueF · Nov 25

Dr. Geoff Heriot at #GDS2021: There is a big role for the #QUAD and other minilaterals in cyberspace @KASonline @#cyberspace @AusIndiaCouncil

Global Dialogue Forum @GlobalDialogueF · Nov 25

Replying to @GlobalDialogueF

.@CENJOWS Director, Lt. Gen Srivastava: Its no more a situation of binary relationship of war or peace with states. There are both state and non state actors involved. Violence is predominant means of coercion. War strategies have become hybrid. #GDSS2021 #cyberspace @KASonline

Add another Tweet

Global Dialogue Forum @GlobalDialogueF · Nov 25

Replying to @GlobalDialogueF

Lt Gen Srivastava: Early warning is impt ingredient of a good defence – but cyber warfare give no signs. Offensive strategies are needed to combat cyber attacks. #GDSS2021 @CENJOWS

Global Dialogue Forum @GlobalDialogueF · Nov 25

George Mikaberidze, CEO, Rosinfokominvest speaks on Digital Sovereignty and Cyberwars as well as Digital Colonialism at #GDSS2021 @KASonline @KASMediaAsia #IndoPacific #cyberspace



Global Dialogue Forum @GlobalDialogueF · Nov 25

Hon'ble Member of Parliament Mr. K.J. Alphons @alphonstourism speaking at the #GDSS2021 @KASonline #cyberspace #IndoPacific



Global Dialogue Forum @GlobalDialogueF · Nov 25

.@SangmaConrad at the #GDSS2021 @CMO_Meghalaya @KASonline @CENJOWS



Conrad Sangma



You Retweeted



Conrad Sangma ✓ @SangmaConrad · Nov 25

Attended the Global Digital Security Summit on Managing Cyberspace in the Indo Pacific. Stressed on the need of cybersecurity in today's digital age and Meghalaya's initiatives of using technology to promote good governance.

@AshwiniVaishnaw

@GlobalDialogueF



Ministry of Electronics & IT



Global Dialogue Forum @GlobalDialogueF · Nov 25

.@ElbitSystemsLtd Lt. Col. Ofer Rotberg: Connection between cyberspace and other domains – space, air, land, maritime all will be connected in the coming years – a multi domain perspective



Global Dialogue Forum @GlobalDialogueF · Nov 25

Dr. Gudrun Wacker @GudrunWacker @SWPBerlin at the #GDSS2021 @KASonline #IndoPacific #Cyberspace



Global Dialogue Forum @GlobalDialogueF · Nov 25

.@Mutchu4

Member of Legislative Assembly, Roing, Arunachal Pradesh: Info and data is not consigned to privileged few, now everyone has access. #Cyberspace is a huge leap for mankind and science fiction has become reality

#IndoPacific
@KASonline





Global Dialogue Forum @GlobalDialogueF · Nov 25

Dr. Kapesa Pfokrelo, North East Christian Uni: COVID has exemplified the importance of cyberconnectivity especially in education sector and small businesses. Connectivity in NE is still a challenge. Cyberspace plays impt role in bridging space between govt & citizens #GDSS2021



1 2 3 4 5



Global Dialogue Forum @GlobalDialogueF · Nov 25

Mr. Navin Singh, IPS spethe Valedictory Address: Cyberspace War - Protecting and Defending India #GDSS2021 @KASonline @CENJOWS #cyberspace #IndoPacific



1 2 3 4 5



Global Dialogue Forum @GlobalDialogueF · Nov 25

We should work towards a Cybersecurity Act - Navin Singh, IPS at #GDSS2021 @KASonline

1 2 3 4 5



Global Dialogue Forum @GlobalDialogueF · Nov 25

.@KASonline Pankaj Madan at the #GDSS2021 #Cyberspace #IndoPacific



1 2 3 4 5

PHOTOS









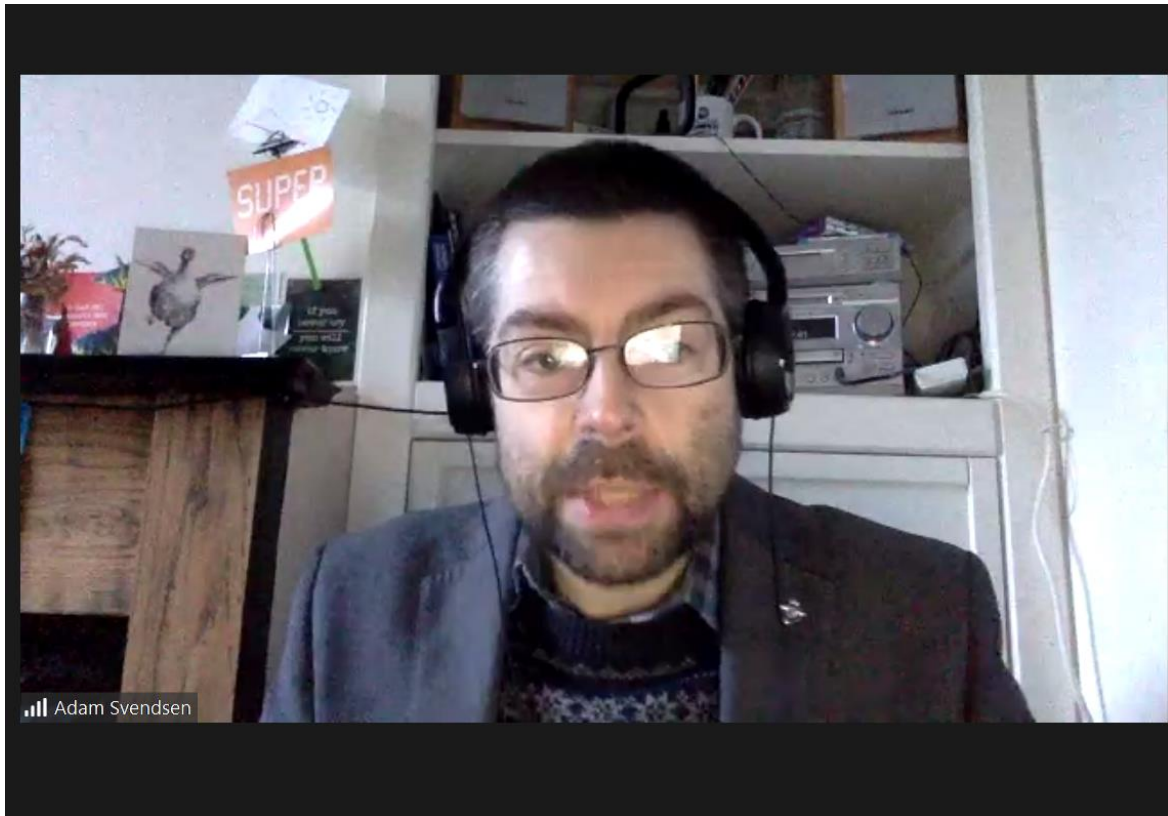














MEDIA COVERAGE

1. <https://www.sentinelassam.com/north-east-india-news/meghalaya-news/meghalaya-chief-minister-conrad-k-sangma-stresses-on-use-of-technology-in-governance-564890>

আজিৰ অসম

সময় প্ৰবাহ

বৰ সৈনিক

হিন্দী সৈনিক

 **The Sentinel**
of this land, for its people

Thursday, 30 Dec 2021

ePaper

HOME LIVE BLOG BREAKING NEWS TOP HEADLINES CITIES NE NEWS SENTINEL MEDIA SPORTS EDUCATION JOBS MORE

New Year 2022 — Here are Some New Year Wishes And Inspirational Quotes For a Good Start Finalization of India-Philippines BrahMos Missile Deal Inching Closer

Home / NE News / Meghalaya News / Meghalaya Chief...

Meghalaya Chief Minister Conrad K. Sangma stresses on use of technology in governance

Meghalaya Chief Minister Conrad K. Sangma has said that technology plays a crucial role in Governance.



Jobs in Assam

- 30 Dec 2021 1:48 PM
NISG Recruitment 2022: Project Manager Vacancy, Job Openings
- 30 Dec 2021 11:56 AM
DC Goalpara Recruitment 2022: Lot Mandal Vacancy, Latest Jobs
- 30 Dec 2021 11:38 AM
Darrang Social Welfare Office Recruitment 2022 - Clinical Psychologist, Sr. Physiotherapist/ Occupational Therapist, Job Opening
- 30 Dec 2021 11:17 AM
CDPO Nazira Recruitment 2022 - Mini Anganwadi Worker, Anganwadi Helper Vacancy, Job Opening
- 29 Dec 2021 1:54 PM
PNRD Assam Recruitment 2022: Management Professionals Vacancy, Job Openings

 By : Sentinel Digital Desk | 28 Nov 2021 11:05 AM



SHILLONG: Meghalaya Chief Minister Conrad K. Sangma has said that technology plays a crucial role in Governance.

The Chief Minister said this on Thursday while delivering his address during the second day of 'The Global Dialogue Security Summit' being held in Shillong.

He also said that technology and IT enabled services has helped in monitoring the different programmes and initiatives of the Government and aided in effective service delivery to the people. 'With the use of technology to monitor pregnant mothers in the state through the 'MOTHER' programme, the Government has been able to increase the institutional deliveries. We will be touching almost 70 percent in the next three years and even the maternal mortality has come down. When it comes to road projects technology and the internet has helped to gather data and monitor the progress of critical road infrastructure being implemented in the State', the Chief Minister said.

Speaking at length on the different aspects of a digitally connected world the Chief Minister also said that reaping the benefits of the information age requires that information networks and systems be stable, reliable, available and trusted adding that the integrity security and stability of cyberspace in general requires concerted action from all.

The Chief Minister also said that Information and technology has opened avenues for self-employment especially for the youth of the region and it is in the best interest that these opportunities are utilised to usher in better economic growth of the region and the country as whole.

2. <https://ukhrultimes.com/global-dialogue-security-summit-held-in-shillong/>

Ukhrul Times

HOME OPINION UKHRUL MANIPUR NORTHEAST COVID-19 FEATURES KNOW YOUR INTENDING MLA MORE

NORTHEAST MEGHALAYA SHILLONG

Global Dialogue Security Summit held in Shillong

Conrad Sangma said that information and technology has opened avenues for self-employment especially for the youth of the region and it is in the best interest that these opportunities are utilised to usher in the better economic growth of the region and the country as a whole.

By UT News Service November 25, 2021 - 8:55pm

Share

f

in

Twitter

WhatsApp

Pinterest



File photo

Shillong: Meghalaya Chief Minister Conrad K Sangma today said that technology plays a crucial role in governance.

The Chief Minister said this while delivering his address during the second day of The Global Dialogue Security Summit being held in Shillong.

He said that technology and IT-enabled services have helped in monitoring the different programmes and initiatives of the Government and aided ineffective service delivery to the people.

“With the use of technology to monitor pregnant mothers in the state through the ‘MOTHER’ programme, the Government has been able to increase the institutional deliveries. We will be touching almost 70 per cent in the next three years and even maternal mortality has come down. When it comes to road projects technology, the internet has helped to gather data and monitor the progress of critical road infrastructure being implemented in the state,” said the Chief Minister.

Speaking at length on the different aspects of a digitally connected world the Chief Minister also said that reaping the benefits of information age requires information networks and systems to be stable, reliable, available and trusted, adding that the integrity, security and stability of cyberspace in general requires concerted action from all.

The Chief Minister also said that information and technology has opened avenues for self-employment especially for the youth of the region and it is in the best interest that these opportunities are utilised to usher in the better economic growth of the region and the country as a whole.

ADVERTISEMENT 002

ADVERTISE YOUR BUSINESS HERE

Reach Us Today

9513511230

ukhrultimes@gmail.com

Connect With Us

f

10,681 Fans

LIKE

Twitter

358 Followers

FOLLOW

Latest

Powerful IED blast in Imphal amid tight security measures ahead of VVIPs visit, no casualty

December 29, 2021 - 8:46pm



Cabinet minister and NPP leader Letpao Haokip joins BJP

December 29, 2021 - 8:44pm



CM N Biren graces cultural session of Makhel Heritage Conclave



57

3. <https://hubnetwork.in/it-enabled-services-have-aided-govt-in-effective-service-delivery-conrad-at-global-dialogue-security-summit-2021/>

[f](#)
[@](#)
[v](#)
[d](#)
[p](#)

[HOME](#)
[NEWS](#)
[GARO NEWS](#)
[STORIES](#)
[VIDEOS](#)
[PODCAST](#)

[NEWS](#)
[DEVELOPMENT](#)
[MEDIATION](#)

IT enabled services have aided govt in effective service delivery: Conrad at Global Dialogue Security Summit 2021

By Hub Network · November 25, 2021 · 182

Shillong, Nov 25: Meghalaya Chief Minister Conrad K. Sangma on Thursday said that technology plays a crucial role in Governance. The Chief Minister said this while delivering his address during the second day of 'The Global Dialogue Security Summit' being held in Shillong.

He said that technology and IT enabled services have helped in monitoring the different programmes and initiatives of the Government and aided in effective service delivery to the people.

"With the use of technology to monitor pregnant mothers in the state through the 'MOTHER' programme, the Government has been able to increase the institutional deliveries. We will be touching almost 70 percent in the next three years and even the maternal mortality has come down. When it comes to road projects technology and the internet has helped to gather data and monitor the progress of critical road infrastructure being implemented in the State," the Chief Minister said.

Speaking at length on the different aspects of a digitally connected world the Chief Minister also said that reaping the benefits of the information age requires that information networks and systems be stable, reliable, available and trusted adding that integrating security and stability of cyberspace in general requires concerted action from all.

The Chief Minister also said that Information and technology has opened avenues for self-employment especially for the youth of the region and it is in the best interest that these opportunities are utilised to usher in better economic growth of the region and the country as whole.

Latest article

Nagaland-o dosgri manderanko sootgalanio jak dongcipa sipairangko taraken sasi onchina dabitoka
December 30, 2021

HNLC bobli doini mande saksu BSF dolna bame on-ae
December 30, 2021

HNLC cadre surrenders before BSF in Meghalaya
December 30, 2021

Nagaland killings: Naga body demands immediate punishment for the accused
December 30, 2021

East Khasi Hills & Ri Bhoi DCs ordered to begin land acquisition process for Shillong-Western Bypass
December 25, 2021

58

4. <https://www.ifp.co.in/meghalaya/technology-plays-a-crucial-role-in-governance-cm-conrad-sangma>

Thursday, 30 December 2021

Imphal Free Press

Covid 19 Northeast Exclusive Education Environment Culture India Videos More

Back


Northeast

Technology plays a crucial role in governance: CM Conrad Sangma

The Meghalaya chief minister addressed the second day of The Global Dialogue Security Summit being held in Shillong.

By NNN/Shillong Updated on 25 Nov 2021, 10:31 pm

WhatsApp Facebook Twitter



Meghalaya Chief Minister Conrad K Sangma (PHOTO: Facebook)

Meghalaya Chief Minister Conrad K Sangma on Thursday said that technology plays a crucial role in governance.

The chief minister said this while delivering his address during the second day of The Global Dialogue Security Summit being held in Shillong. He said that technology and IT-enabled services have helped in monitoring the different programmes and initiatives of the Government and aided ineffective service delivery to the people.

"With the use of technology to monitor pregnant mothers in the state through the 'MOTHER' programme, the Government has been able to increase the institutional deliveries. We will be touching almost 70 per cent in the next three years and even maternal mortality has come down. When it comes to road projects technology and the internet has helped to gather data and monitor the progress of critical road infrastructure being implemented in the State", the Chief Minister said.

Speaking at length on the different aspects of a digitally connected world the Chief Minister also said that reaping the benefits of the information age requires that information networks and systems be stable, reliable, available and trusted adding that the integrity, security and stability of cyberspace, in general, requires concerted action from all.

The Chief Minister also said that Information and technology has opened avenues for self-employment especially for the youth of the region and it is in the best interest that these opportunities are utilised to usher in the better economic growth of the region and the country as a whole.

First published: 25 Nov 2021, 10:31 pm

Tags: governance technology mother programme Meghalaya Chief Minister Conrad K Sangma

Top Stories

India's Omicron cases mount to 961; Punjab reports first...

IFP Bureau • 30 Dec 2021, 12:43 pm

Disturbed Area status not warranted as no aggravated...

IFP Bureau • 30 Dec 2021, 2:52 am

Manipur government issues new COVID-19 SOP; night...

IFP Bureau • 29 Dec 2021, 7:28 pm

Exclusive

That man from Tanzania

IFP Bureau • 30 Dec 2021, 2:38 am

The time gap in detection

IFP Bureau • 29 Dec 2021, 2:35 am

Death in pre-poll violence and malpractices

RK Nimal • 29 Dec 2021, 4:39 am

Living as 'anonymous persons', female sex worker...

Phurailatpam Keny Devi • 26 Dec 2021, 8:27 pm

59

5. <http://www.uniindia.com/technology-plays-a-crucial-role-in-governance-meghalaya-cm/east/news/2574333.html>

UNI
BREVITY
ACCURACY
SPEED

United News of India
India's Multi Lingual News Agency

Thursday, Dec 30 2021 | Time 17:35 Hrs(IST)



अल्पसंख्यक कार्य मंत्रालय
भारत सरकार

हुनर हाट

दस्कारो, शिल्पकारो, कारीगरो
के स्वदेशी उत्पादन का प्रामाणिक प्लेटफॉर्म

www.minorityaffairs.gov.in

Home News Photo Hindi Kannada Urdu f About UNI Contact us JOBS PRESS RELEASES Type your keyword Login

India World Sports Business & Economy Entertainment States Parliament

States »

East

Posted at: Nov 25 2021 8:56PM



Technology plays a crucial role in governance : Meghalaya CM

Shillong, Nov 25 (UNI) Meghalaya Chief Minister Conrad K. Sangma on Thursday said that technology plays a crucial role in Governance.

Delivering his address during the second day of The Global Dialogue Security Summit being

Tags: #Technology plays a crucial role in governance : Meghalaya CM **Please log in to get detailed story.**

UNI Photo



LUCKNOW, DEC 30 (UNI)- Newly appointed Uttar Pradesh Chief Secretary Durga Shankar Mishra taking over charge from the outgoing Chief Secretary Rajendra Kumar Tiwari in

6. <https://www.facebook.com/TeamEP/posts/global-dialogue-security-summit-2021shillong-25-november-meghalaya-chief-minister/4714876108572667/>

**Eastern Panorama**

November 25 · 🌐

...

Global Dialogue Security Summit 2021

Shillong 25 November: Meghalaya Chief Minister Conrad K. Sangma today said that technology plays a crucial role in Governance.

The Chief Minister said this while delivering his address during the second day of The Global Dialogue Security Summit being held in Shillong.

He said that technology and IT enabled services has helped in monitoring the different programmes and initiatives of the Government and aided in effective service delivery to the people.

'With the use of technology to monitor pregnant mothers in the state through the 'MOTHER' programme, the Government has been able to increase the institutional deliveries. We will be touching almost 70 percent in the next three years and even the maternal mortality has come down. When it comes to road projects technology and the internet has helped to gather data and monitor the progress of critical road infrastructure being implemented in the State', the Chief Minister said.

Speaking at length on the different aspects of a digitally connected world the Chief Minister also said that reaping the benefits of the information age requires that information networks and systems be stable, reliable, available and trusted adding that the integrity security and stability of cyberspace in general requires concerted action from all.

The Chief Minister also said that Information and technology has opened avenues for self-employment especially for the youth of the region and it is in the best interest that these opportunities are utilised to usher in better economic growth of the region and the country as whole.



ABOUT THE PARTNERS

Global Dialogue Forum (GDF)

Global Dialogue Forum (GDF) is an independent think tank which publishes the foreign policy journal Global Dialogue Review (GDR).

GDF, without ties to big business or government, is a non-profit trust that is carving out an intellectual space over a range of geopolitical issues concerning the Developing World, from security to the environment to the economy to law.

Having grown out of roots in a country with a colonial past, a formidable present and a greatly promising future, GDF believes it has a legitimacy to seek out and collaborate with similar societies across the world.

GDF's objectives are to engage every stakeholder in society - from the state to those at grassroots levels - in unfettered debate and discussion, as well as through seminars and conferences.

Through Global Dialogue Advisory & Advocacy, it will provide honest and authoritative assessment of country and corporate risk; and to help develop, through partnerships with teaching institutions, a generation of influencers to shape an equitable future, as well as to sensitise the vulnerable, especially women, in conflict and other contentious zones.

This work will be done mainly through the Global Dialogue Remote Learning Academy.

It will also publish analyses that are sensitive to the concerns and cultures of emerging societies at the heart of GDF. To this end, it will run internship and research programmes as well as online certificate courses.

GDF has already done what no other Indian think tank has been able to do so far - regularly organise major conferences overseas, from China to the UK. In London, last November, our conference on India's suitability as a global centre for dispute resolution was in partnership with UK's premier think tank, Chatham House, the Royal Institute of International Affairs.

In China, no Indian entity has ever conducted a conference on the scale GDF/GDR did in 2016, with key partners, the Communist Party, the Chinese Academy of Social Sciences and the People's Liberation Army (PLA), whose respect for us is reflected in their participation in the annual Global Dialogue Security Summits.

GDF plans joint academic centres with eminent local partners in China, Kazakhstan, Russia, Indonesia, Ethiopia and Sweden. It believes China, India, Indonesia, Central Asia, Russia and Africa will define the global geopolitical landscape of the 21st Century.

Its academy will focus on the role of women in conflict resolution, climate change, the global economy and international law. It will conduct live, interactive courses with distinguished speakers from around the world to a global classroom of students in various certificate courses.

Konrad-Adenauer-Stiftung (KAS)

The Konrad-Adenauer-Stiftung (KAS) is a political foundation.

Established in 1955 as “Society for Christian-Democratic Civic Education”, in 1964 the Foundation proudly took on the name of Konrad Adenauer, the first Chancellor of the Federal Republic of Germany.

With 16 regional offices in Germany and over 120 offices abroad, the Konrad Adenauer Foundation is committed to achieving and maintaining peace, freedom and justice through political education.

We promote and preserve free democracy, social market economy, and the development and consolidation of the value consensus. We focus on consolidating democracy, the unification of Europe and the strengthening of transatlantic relations, as well as development cooperation.

The leitmotif of the Konrad Adenauer Foundation — "Germany. The next chapter" — is supported by a thematic focus.

With the focus on three main topics — Innovation, Security and Representation and Participation — it is quite clear the topics Konrad Adenauer Foundation will prioritise in the coming years.

KAS cooperates with governmental institutions, political parties and civil society organisations, building strong partnerships along the way. In particular, it seeks to intensify political cooperation in the area of development cooperation on the foundation of our stated objectives and values.

Together with our partners, we aim to make a significant contribution to the creation of a global order that empowers every country to determine its own developmental priorities and destiny in an internationally responsible manner.

The Konrad-Adenauer-Stiftung has organised its program priorities in India into five working areas:

1. Foreign and Security Policy
2. Economic, Climate and Energy Policy
3. Rule of Law
4. Political Dialogue focussed on Social and Political Change
5. Media and Youth.

The India Office of the Konrad Adenauer Foundation takes great pride in its cooperation with Indian partner institutions who implement jointly curated projects and programmes.

Centre For Joint Warfare Studies (CENJOWS)

CENJOWS, an independent think tank, was established in 2007, to promote “Integrated National Power” and “to suggest alternatives” for its application. Its vision is to be a premier think tank, promoting jointness, integration and transformation in the Indian Armed Forces. It accords priority to free dialogue and discussion on all issues having a bearing on “Joint Warfare” and formulation of related policy options. It endeavours to shape policy and doctrines related to synergetic application of national power, by facilitating studies and wider discourse.

It seeks to engage Indian and foreign institutions with common objectives, to promote mutual understanding and cooperation in joint warfare, strategic studies, doctrines and concepts. It undertakes and organises analytical studies, environmental scans, scenario building, round table and panel discussions, webinars and seminars; with participation from policy makers, armed forces training institutions, academia, scientific community and think tanks.

CENJOWS has been enhancing awareness amongst service officers on Defence and Security by harnessing domain expertise of experts and veterans. It promotes knowledge sharing through publications like SYNERGY, its bi-annual journal, monographs, issue briefs, occasional papers and books.

