INSTITUTE FOR DEFENCE STUDIES & ANALYSES
रक्षा अध्ययन एवं विश्लेषण संस्थान

IPAG
The Institute for Policy, Advocacy, and Governance

IDSA-IPAG International Conference on

Digital Age & Cyber Space

Maximizing Benefits, Minimizing Risks, Unleashing Creativity

Conference Report & Compilation of Session Proceedings

Unlocking Potential
Securing Connectivity

Knowledge Partner

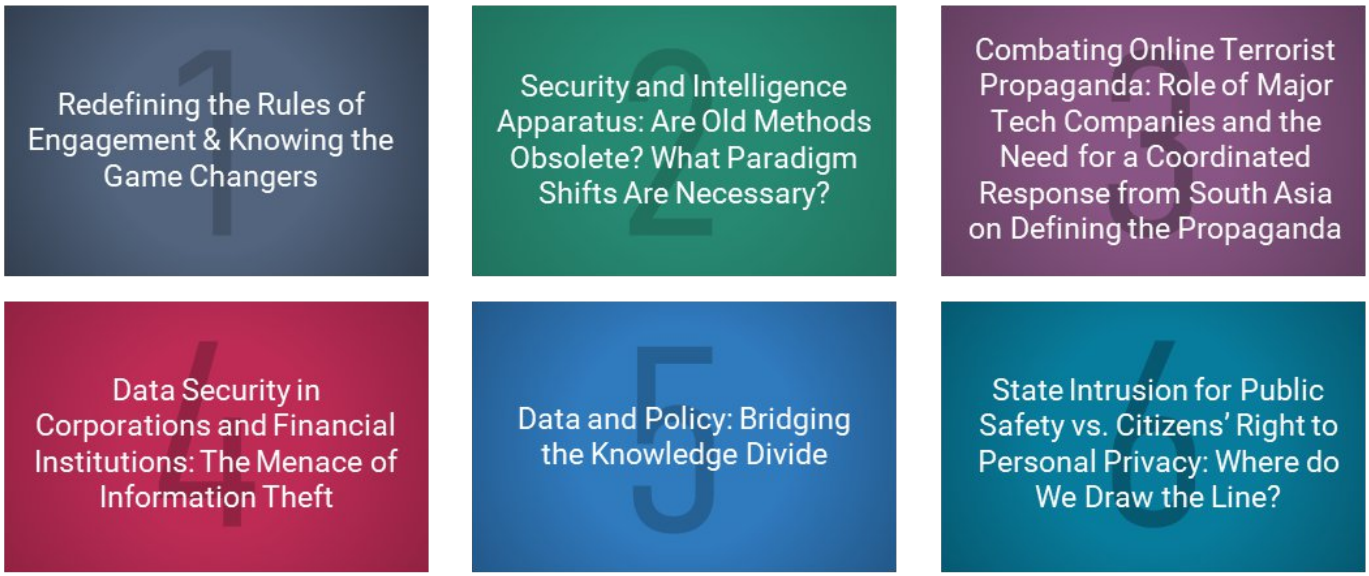
IDRC | CRDI Technical Partner

August 28-29, 2018
New Delhi, India

Executive Summary

The digital revolution during the last three decades has created unprecedented levels of connectivity for mankind. While this has led to an enhancement in lifestyle and rapid economic development for many, the increased connectivity has also brought along significant risks both in the cyber and real world. The rising instances of online radicalisation and data breaches highlight some of the risks created in cyberspace.

3 Against this background, The Institute for Defence and Security Analysis (IDSA) a think tank affiliated with the Ministry of Defence, Government of India and The Institute for Policy, Advocacy, and Governance (IPAG), an international think tank with presence in South Asia (Bangladesh), Asia Pacific (Australia), Europe (Austria) and the MENA region (UAE) jointly organised the International Conference on ***"Digital Age and Cyber Space: Maximizing Benefits, Minimizing Risks, Unleashing Creativity"*** *on August 28-29, 2018 in New Delhi, India. The two-day conference had*



the following six thematic sessions:

The Conference had high level representation from the Government of India which included Amitabh Kant, CEO, NITI Aayog and Dr. Gulshan Rai, National Cyber Security Coordinator, Prime Minister's Office, Government of India. The conference was participated by international experts from diverse backgrounds including the government officials, policy makers, industry players, academia, civil society, and media. As such, the conference provided a platform to all the stakeholders in the cyber industry to engage in discussions and deliberate upon the challenges

facing cyberspace, and finally come up with recommended policies & strategies to combat the threat of online radicalisation and data breaches.

Table of Contents

Conference Agenda

Date: August 28-29 (Tue-Wed), 2018
Location: Auditorium, IDSA Campus
1, Development Enclave, (near USI), New Delhi 110010, India

Day 1	
Inaugural Session	
9.00 am – 9.30 am (30 Minutes)	**Registration**
9.30 am – 10.15 am (45 Mins)	**Event Schedule**
9.30 am – 9.35 am (5 Minutes)	**Welcome Address:** **Maj Gen Alok Deb, SM, VSM (Retd.),** Deputy Director General, IDSA, India
9.35 am – 9.40 am (5 Minutes)	**Opening Remarks:** **Syed Munir Khasru**, Chairman, IPAG
9.40 am – 9.55 am (15 Minutes)	**Keynote Address:** **Amitabh Kant**, CEO, Niti Aayog (National Institution for Transforming India), Government of India
9.55 am – 10.05 am (10 Minutes)	**Audio-Visual**
10.05 am – 10.10 am (5 Minutes)	**Group Photo**
10.10 am – 10.30 am (20 Minutes)	**Coffee Break**

Session I: Redefining the Rules of Engagement & Knowing the Game Changers	
10.30 am – 12.00 pm (90 mins)	
10.30 am – 10.50 am (10 mins each)	**Moderator:** **Syed Munir Khasru,** Chairman, IPAG **Key Note Presentations:** 1. **Richard Wike,** Director, Global Attitudes Research, Pew Research Center, US 2. **Dr. Stephen Tankel,** Associate Professor, American University & Adjunct Senior Fellow, Center for a New American Security, Washington D.C., US
10.50 am – 11.00 am (5 mins each)	**Panel Discussion:** **Panelists:** 1. **Ambassador Latha Reddy,** Co-Chair of the Global Commission on the Stability of Cyberspace, India 2. **Dipakshi Mehandru,** Senior Advisor - Government Affairs and Public Policy, Dell
11.00 am – 11.30 am (30 mins)	**Intra Panel Discussion**
11.30 am – 12.00 pm (30 mins)	**Q&A and Open Floor Discussion**
Session II: Security and Intelligence Apparatus: Are Old Methods Obsolete? What Paradigm Shifts Are Necessary?	
12.00 pm – 1.30 pm (90 mins)	
12.00 pm – 12.20 pm (10 mins each)	**Moderator:** **Maj Gen Alok Deb, SM, VSM (Retd.),** Deputy Director General, IDSA, India **Key Note Presentation:** 1. **Farah Pandith,** Adjunct Senior Fellow, Council on Foreign Relations (CFR) & Head of Strategy, Institute of Strategic Dialogue (ISD), UK 2. **Andrew Balmaks,** Chairman, Institute for Regional Security (IRS), Australia
12.20 pm – 12.30 pm (5 mins each)	**Panel Discussion:** **Panelists:** 1. **Benjamin Ang**, Senior Fellow, S. Rajaratnam School of International Studies

	(RSIS), Singapore 2. **KPM Das**, India Cybersecurity and Trust Officer, CISCO
12.30 pm – 1.00 pm (30 mins)	**Intra Panel Discussion**
1.00 pm – 1.30 pm (30 mins)	**Q&A and Open Floor Discussion**
1.30 pm – 2.30 pm (60 Minutes)	**Lunch**
Session III: Combating Online Terrorist Propaganda: Role of Major Tech Companies and the Need for a Coordinated Response on Defining the Propaganda	
2.30 pm – 4.00 pm (90 minutes)	
2.30 pm – 2.50 pm (10 mins each)	**Moderator:** **Shruti Pandalai**, Fellow, IDSA, India **Key Note Presentation:** 1. **Scott Carpenter,** Managing Director, Jigsaw, Google, US 2. **Jessie Lowry Francescon**, Senior Advisor of CVE Communications, U.S. State Department & Director of Dialogue & Communication, Hedayah Centre, US **Panel Discussion:**
2.50 pm – 3.00 pm (5 mins each)	**Panelists:** 1. **Serge Stroobants,** Director of Operations for Europe and the MENA Region, Institute for Economics and Peace, Belgium 2. **Kavitha Kunhi Kannan,** Public Policy Manager, Facebook-India, South Asia and Central Asia
3.00 pm – 3.30 pm (30 mins)	**Intra Panel Discussion**
3.30 pm – 4.00 pm (30 mins)	**Q&A and Open Floor Discussion**
Parallel Session: Workshop by CISCO (Invitation Only) **Digital Convergence in The Battlefield: A Cyber View**	
2:30 pm – 4:00 pm (90 mins)	CISCO

	Speaker: **KPM Das**, India Cybersecurity and Trust Officer, CISCO
(15 mins)	***Security Solutions for Defence: The Digital Battlefield and its Components***
(25 mins)	***Security Solutions for Defence: Security Architectures for Defence***
(15 mins)	***Building Security Competencies: Cyber Range***
(20 mins)	***Executing Security Operations: SOC for the Digital Force***
(15 mins)	***Threat Intelligence: TALOS and Proposition for CERT-Army/Navy/AF***
4.00 pm– 4.15 pm (15 mins)	**Coffee Break**
Session IV: Data Security in Corporations and Financial Institutions: The Menace of Information Theft	
4.15 pm – 5.45 pm (90 Mins)	
	Moderator: **Amit Sharma,** Additional Director in the Office of the Scientific Advisor of Defence Minister, Defence Research and Development Organization (D.R.D.O), Ministry of Defence, Government of India
4.15 pm – 4.35 pm (10 mins each)	**Key Note Presentation:** 1. **Dr. John Mallery,** Research Scientist, Computer Science and AI Laboratory Massachusetts Institute of Technology (MIT), US 2. **Damien Manuel**, Director - Cyber Security Research and Innovation Centre (CSRI), School of Information Technology, Faculty of Science Engineering and Built Environment, & Chairman – Australian Information Security Association (AISA)
4.35 pm – 4.45 pm (5 mins each)	**Panel Discussion:** **Panelists:** 1. **Omar Sherin,** Director of Cyber Security, E&Y-MENA, Qatar 2. **Ashish Sonal**, CEO, Orkash, India
4.45 pm – 5.15 pm (30 mins)	**Intra Panel Discussion**
5.15 pm – 5.45 pm	**Q&A and Open Floor Discussion**

(30 mins)	

Day 2	
10.00 am – 10.30 am (30 Mins)	**Special Key Note Speaker:** **Dr. Gulshan Rai,** National Cyber Security Coordinator, Prime Minister Office, Government of India
Session V: Data and Policy: Bridging the Knowledge Divide	
10.30 am – 12.00 pm (90 Mins)	
10.30 am – 10.50 am (10 mins each)	**Moderator:** **Dr. Madan M. Oberoi**, Special Commissioner of Police, (Special Cell and Technology Cell), Delhi Police, India **Key Note Presentation:** 1. **Klon Kitchen,** Senior Research Fellow, Technology, National Security and Science Policy, The Heritage Foundation, US 2. **Puneet Kukreja,** Partner, Cyber Advisory and Threat Intelligence, Deloitte, Australia
10.50 am – 11.00 am (5 mins each)	**Panel Discussion:** **Panelists:** 1. **Pukhraj Singh,** CTO, Bhujang, India 2. **Rafiqul Islam,** Lead Analyst, Cyber Initiative, IPAG
11.00 am – 11.30 am (30 mins)	**Intra Panel Discussion**
11.30 am – 12.00 pm (30 mins)	**Q&A and Open Floor Discussion**

Parallel Session: Workshop by Facebook (Invitation Only)	
Facebook Community Standards Roundtable	
10.30 am – 12.00 pm (90 Mins)	
	Speakers: 1. **Kavitha Kunhi Kannan** Public Policy Manager (India, South Asia & Central Asia), Facebook 2. **Varun Reddy,** Public Policy Manager, (Content), Facebook
12.00 pm – 12:15 pm (15 mins)	**Coffee Break**
Session VI: State Intrusion for Public Safety vs. Citizens' Rights to Personal Privacy: Where do we Draw the Line?	
12.15 pm – 1.45 pm (90 Mins)	
12.15 pm – 12.35 pm (10 mins)	**Moderator:** **Dr. Sunil Agarwal**, Deputy Director, Cyber Division, National Security Council Secretariat (NSCS), Government of India **Key Note Presentation:** 1. **Syed Munir Khasru,** Chairman, IPAG 2. **Jamil N. Jaffer,** Adjunct Professor, National Security Institute (NSI) Founder, and Director, National Security Law & Policy Program, Antonin Scalia Law School, George Mason University, US
12.35 pm – 12.45 pm (5 mins each)	**Panel Discussion:** **Panelists:** 1. **Albana Shala,** Chair, UNESCO International Programme for the Development of Communication (IPDC) Council, France 2. **Munish Sharma,** Consultant, IDSA
12.45 pm – 1.15 pm (30 mins)	**Intra Panel Discussion**
11.15 pm – 1.45 pm (30 mins)	**Q&A and Open Floor Discussion**
1:45 pm – 2:45 pm (60 mins)	**Closing Lunch**

List of Speakers

Amitabh Kant
CEO, Niti Aayog (National Institution for Transforming India),
Government of India

Dr. Gulshan Rai
National Cyber Security
Coordinator
Prime Minister's Office, India

Maj Gen Alok Deb, SM, VSM (Retd.)
Deputy Director General, Institute for
Defence Studies and Analyses (IDSA), India

Syed Munir Khasru
Chairman
The Institute for Policy, Advocacy, and Governance (IPAG)

Session I: Redefining the Rules of Engagement & Knowing the Game Changers

Moderator

Syed Munir Khasru
Chairman
The Institute for Policy, Advocacy, and Governance (IPAG)

Key Note Speakers

Richard Wike
Director of Global Attitudes Research
Pew Research Center
Washington D.C., US

Dr. Stephen Tankel
Associate Professor, American University
Adjunct Senior Fellow, Center for a New American Security
American University, US

Panelists

Latha Reddy
Co-Chair of the Global Commission on the Stability of Cyberspace
Bangalore, India

Dipakshi Mehandru
Senior Advisor, Government Affairs and Public Policy, Dell Inc.

Session II: Security and Intelligence Apparatus: Are Old Methods Obsolete? What Paradigm Shifts Are Necessary?

Moderator

Maj Gen Alok Deb, SM, VSM (Retd.)
Deputy Director General
Institute for Defence Studies and Analyses (IDSA), India

Key Note Speakers

Farah Pandith
Adjunct Senior Fellow, Council on Foreign Relations (CFR) &
Head of Strategy, Institute of Strategic Dialogue
London, United Kingdom

Andrew Balmaks
Chairman, Institute for Regional Security
Canberra, Australia

Panelists

Benjamin Ang
Senior Fellow
Centre of Excellence for National Security (CENS) & Rajaratnam School of International Studies (RSIS)
Singapore

KPM Das
India Cybersecurity Trust Officer
CISCO
Bangalore, India

Session III: Combating Online Terrorist Propaganda: Role of Major Tech Companies and the Need for a Coordinated Response on Countering the Propaganda

Moderator

Shruti Pandalai
Fellow, IDSA

Key Note Speakers

Scott Carpenter
Managing Director, Jigsaw, Google
Adjunct Scholar, Washington Institute for Near East Policy
New York, US

Jessie Lowry Francescon
Senior Advisor of CVE Communications, US State Department &
Director of Dialogue & Communication, Hedayah Centre, Abu Dhabi, UAE

Panelists

Serge Stroobants
Director of Operations for Europe and the MENA Region, Institute for Economics and Peace, Brussels, Belgium

Kavitha Kunhi Kannan
Public Policy Manager-India, South Asia & Central Asia
Facebook
New Delhi, India

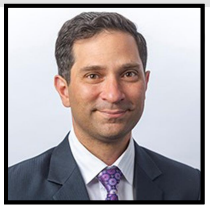
Session IV: Data Security in Corporations and Financial Institutions: The Menace of Information Theft

Moderator

Amit Sharma
Additional Director in the Office of the Scientific Advisor of Defence Minister, Defence Research and Development Organization (D.R.D.O), Ministry of Defence, Government of India

Key Note Speakers

Prof. John C. Mallery
Research Affiliate
MIT Computer Science & Artificial Intelligence Laboratory
Massachusetts, Boston, US



Damien Manuel
Director, Cyber Security Research and Innovation Centre (CSRI), School of Information Technology, Faculty of Science Engineering and Built Environment, Deakin University & Chairman, Australian Information Security Association (AISA)
Melbourne, Australia

Panelists

Omar Sherin
Cyber-Security Director
Ernst and Young, MENA Region
Doha, Qatar

Ashish Sonal
CEO, Orkash
India

Session V: Data and Policy: Bridging the Knowledge Divide

Moderator

Dr. Madan M Oberoi
Director
Special Commissioner of Police (Special Cell and Technology Cell)
Delhi Police, India

Key Note Speakers

Klon Kitchen
Senior Research Fellow for Technology, National Security, and Science
The Heritage Foundation
Washington D.C., US

Puneet Kukreja
National Lead Partner -Cyber Australian Financial Services Data Privacy and Protection, Deloitte, Melbourne, Australia

Panelists

Rafiqul Islam
Lead Analyst
Cyber Initiative
IPAG

Pukhraj Singh
CTO, Bhujang
Gurgaon, India

Session VI: State Intrusion for Public Safety vs. Citizens' Rights to Personal Privacy: Where do we Draw the Lines?

Moderator

Dr. Sunil Agarwal
Deputy Director, Cyber Division
National Security Council Secretariat (NSCS)
Government of India, New Delhi, India

Key Note Speakers

Syed Munir Khasru
Chairman
The Institute for Policy, Advocacy, and Governance (IPAG)

Jamil N. Jaffer
Adjunct Professor, NSI Founder & Director,
National Security Law & Policy Program
Antonin Scalia Law School,
George Mason University ,Virginia, US

Panelists

Albana Shala
Chair of the International Programme for the Development of Communication (IPDC), UNESCO, Paris, France

Munish Sharma
Consultant
IDSA

Background

The digital, age in the 21st century has rapidly shifted the traditional industry processes to an era dominated by digital systems and information technology. Human beings today are more connected, not only among each other, but also with all their day-to-day devices. Equipped with artificial intelligence, machines have become more intuitive, while gradually bridging the differences between humans and devices. While this has led to an enhancement in lifestyle and rapid economic development for many, the increased connectivity has also brought along significant risks both in the cyber world and the real world.

The internet has enabled terror outfits to connect to a large number of people and propagate their misleading agendas. In many unfortunate instances, the internet has provided opportunities to people with ill intentions to prey on a wider population from even the comfort of their homes, seen most evidently in the form of online radicalization, particularly of the younger population. Not only this, as sensitive user data becomes widely available, the risk of cybercrimes, financial scams and data breaches are posing challenges to governments and institutions.

Unless there is a concerted effort, in participation of the key stakeholders, to effectively respond to such online methods of negative engagements with a comprehensive counter-strategy, such incidents are likely to continue hurting innocent people around the world. To combat the threat of online radicalisation and cyber security breaches, it is imperative that the knowhow in the critical issues of cyberspace is shared, leveraged and distributed among the experts, policymakers and practitioners. Further, cyberspace is facing the challenge of formulating important strategies and policy decisions about the development of its fundamental principles including security, freedom, governance, human rights and, norms and ethics.

Against this background, The Institute for Defence and Security Analysis (IDSA) a think tank affiliated with the Ministry of Defence, Government of India and The Institute for Policy, Advocacy, and Governance (IPAG), an international think tank with presence in South Asia (Bangladesh), Asia Pacific (Australia), Europe (Austria) and the MENA region (UAE) jointly organised the International Conference on ***"Digital Age and Cyber Space: Maximizing Benefits, Minimizing Risks, Unleashing Creativity"*** on August 28-29, 2018 in New Delhi, India that brought together major stakeholders from the industry to deliberate, discuss, and debate upon the challenges of online radicalisation and cyber security breaches in the age of digitalisation and social media, and to chart out a set of pragmatic recommendations for the policy makers for effectively responding to such threats. The conference provided a platform for the multi-stakeholder engagement in participation of the policy makers, industry players, civil society and academia for generating discussion on how to collectively counter this global menace.

Objectives of the International Conference

- To understand the process of radicalization and identify multifarious pathways that lead to both online and offline radicalization.
- To recognize the importance of adjusting the counter radical responses to the paradigm shifts in the nature and forms of terrorism and to identify measures needed for addressing new challenges.
- To collaborate among the major industry representatives to build effective strategies to counter extreme radicalism.
- Facilitate Multi-stakeholder engagement.
- To identify risks, analyze costs and assess implications of cyber security breaches and to use technological innovations to tackle the threat.
- To promote understanding and discuss ways to bridge the knowledge gap among the public and the private entities.
- To discuss ways through which a balance can be maintained between the conflicting issues of public safety and citizen's rights.

Thematic Sessions of the Conference

10 Key Recommendations

To address the issue of online radicalization, there is a need to identify the game changers, both positive and negative, in the cyber world cutting across disciplines and offering holistic perspectives. There is a need to connect technical sciences with social sciences to combat the menace of online radicalization and develop effective counter narrative strategies by considering various perspectives, including psychological and anthropological.

For building resilience program against online radicalisation, more information should be shared amongst all the stakeholders and special focus should be given to children and the younger population. A cultural understanding of being a good internet citizen should also be created.

As the nature of means of radicalization are highly localized and individualistic, it is imperative to understand the local context and to use psychological and behavioral approaches for building effective counter narrative strategies.

There is a need to have a comprehensive view while designing security technology with perspectives from businesses, human element, technology, systems, ethics and norms, and law & regulation.

Strategies to secure cyberspace cannot be solved at the policy level only and requires multi-stakeholder engagement amongst the policy makers, tech-giants, intelligence units, civil society and academia. The responsibilities should be shared amongst all the stakeholders and they should come together to address the challenges facing cyberspace.

The civil society can play a vital role in bridging the divide between government and industry through translation and policy innovation.

Existing surveillance programs should be modernised to strike a balance between ensuring security and protecting privacy.

Encryption technology, which is the core of privacy, is also being increasingly used as communication channels to launch terrorist operations. Thus, the benefits and challenges of such technology need to be identified and the global community should reach a consensus to address these challenges.

There is a need for greater international cooperation in internet governance and cyberspace addressing the issues of cybercrime and online radicalization by engaging stakeholders and proposing norms and policies that would guide and govern both the state and non-state actors in cyberspace.

The recent trends in cyberspace related with the issues of privacy, jurisprudence and the legal framework, and the issues of data localisation, ownership and sovereignty are showing a shift away from the notion of open and transparent internet. The policy framework should help strengthen the concept of single cyberspace, and help create a better nation with social prosperity, more wealth and better education.

Organisers of the Conference

Institute for Defence Studies and Analyses (IDSA)

The Institute for Defence Studies and Analyses (IDSA) is affiliated with the Ministry of defence, Government of India and is a non-partisan, autonomous body dedicated to objective research and policy relevant studies on all aspects of defence and security. Its mission is to promote national and international security through the generation and dissemination of knowledge on defence and security-related issues. IDSA has a well-qualified multi-disciplinary research faculty drawn from academia, defence forces and the civil services, representing a diversity of views in the areas of international relations, regional connectivity and security. Through its experienced academia and widespread network, IDSA is well positioned to provide the knowledge and other forms of support for the conference.

The Institute for Policy, Advocacy and Governance (IPAG)

The Institute for Policy, Advocacy, and Governance (IPAG) is an independent, international think tank with focus on international relations, security & strategic affairs, economic development & trade, regional cooperation & integration, migration & resettlement, power & energy, sustainable development and green growth. Starting out of Dhaka, Bangladesh, IPAG has expanded its presence in the Asia-Pacific (Melbourne, Australia), Europe (Vienna, Austria), and Middle-East and North Africa (Dubai, UAE). IPAG maintains global outreach through collaboration with leading think tanks, research institutes and policy bodies around the world. IPAG has generated considerable research, hosted multiple conferences and training programs and disseminated information on international relations and security affairs. IPAG's quality work has enabled it to make successful interventions in South Asia and beyond, extending its positive impact towards the G20 nations as well. As one of the youngest international think tanks in the world, in the very 1st year of Global Ranking, IPAG has been ranked 42nd among the top 132 in the category

"International Development" & 26th among the top 105 in 'Think Tank to Watch in 2018'. The Global Ranking is done by the Think Tank and Civil Societies Program (TTCSP), Lauder Institute, University of Pennsylvania, US covering around 7,500 think tanks of the world. IPAG has substantial knowledge base and skills in formulating policies through research and stakeholder consultation to counter the impacts of radicalization.

Partners to the Conference

IPAG thanks Facebook India, International Development Research Centre (IDRC)-Asia Regional Office, and Dell EMC for joining the IDSA-IPAG International Conference on Cybersecurity and extending their support to the event.

Facebook, one of the leading social media websites in the world and a significant stakeholder in the cyber industry was Knowledge Partner to the Conference.

IDRC, an organization that promotes research in developing countries and supports leading thinkers who advance knowledge and solve practical development problems, was Technical Partner to the Conference.

Dell EMC, a leading corporation in storing, managing, protecting and analyzing data, was also a Partner to the event.

The contribution and participation of the partners made the entire exercise value additive and were vital in making the conference a success. Their support is much appreciated by IPAG.

The International Conference

The two-day International Conference commenced with an Inaugural Ceremony attended by Amitabh Kant, the CEO of NITI Aayog, Maj Gen Alok Deb, SM, VSM (Retd.), Deputy Director General, IDSA, Syed Munir Khasru, Chairman, IPAG and moderated by Shruti Pandalai, Associate Fellow, IDSA.

This document collates discussions and deliberations from the six sessions which brought together different stakeholders including the international experts, industry players, policy makers, practitioners, academicians and civil society organisation, and makes policy recommendations in formulating the future of cyberspace.

Inaugural Ceremony

Maj Gen. Alok Deb (Retd.), Deputy Director General, IDSA, delivered the Welcome Address and set the context for the two-day International Conference. He highlighted that the variety of tools that the cyberspace provides for influencing minds are growing by the day; as a consequence of which, the whole population is being swayed by the radical ideas and young people are being influenced into giving up on certain lifestyle to fight for malign causes that espouse what human civilisation negates. Hence, he asserted, this is the time we need to discuss these issues in great detail and depth. He referred to the Comprehensive UNESCO Study of 2017 on the issue of cyber security which noted that the governments which endorse the concept of freedom of expression are opting to invest in primary prevention through education of the public at large and young people in particular. Various nations in West Asia and North Africa have already begun programmes to target the youth directly on the premise that such literacy can positively empower youth participation in the marginalisation of extremism if not its containment.

The study further noted that radicalisation of young people online is yet to attract critical mass of studies for credible research. He also highlighted similar problems faced by India and stated that despite the percentage of terrorist cases in comparison to the Indian population being low, the National Investigation Agency has been very proactive and has diligently followed upon various cases. However, there is much to be done in research and analyse in this field, and various preventive measures are yet to be ascertained. Additionally, he highlighted the conflicting issues of the need for law and cyber enforcement agencies to analyse digital footprints of citizens while respecting the right of individual for absolute privacy. Finally, he welcomed all the participants to the conference and said that the value of the IDSA-IPAG Conference can hardly be overemphasized and by sharing of views by practitioners of security and also companies in the business of digital technology, will enable us to understand these issues better.

Syed Munir Khasru, Chairman, IPAG in his Opening Remarks, thanked IDSA and all the participants for joining IPAG in the International Conference. He also thanked Facebook -the Knowledge Partner and IDRC Canada -the Technical Partner, and Dell EMC who together contributed to the event. He then elaborated on how technological advancements and digitalisation have affected almost every aspect of our lives. He highlighted that today, 4 billion people have access to Internet which has jumped from 2 billion in 2015. The trade in ICT goods and services have crossed 2 trillion and have been employing approximately 100 million people. The share of global ICT GDP is more than $5 trillion and only three countries across the world has a higher GDP - US, China and Japan. He further emphasised that while technology has brought immense opportunities and empowerment among people, it also has created significant risks. Every 39-40 second, there is a hacking attack and 43% of the targets are small businesses, and the big. It has been calculated that by 2021, the cost of cyber related crime will cross almost 6 trillion and by the same year, the amount needed to tackle would be almost 1 trillion. Therefore, he mentioned that the technology has come up with lot of inequalities and

security challenges and thus we collectively need to start thinking about it ahead of time. IDSA-IPAG International Conference on Cyber Security is one small step towards that collective commitment in the region.

Keynote Address by Amitabh Kant, the CEO, NITI Aayog, Government of India

Amitabh Kant, in his Keynote Address in the Inaugural Session offered key insights into Government of India's major programmes and schemes built on digitization and the need to build on the new opportunities while simultaneously addressing the risks of technology. He emphasised that digitisation brings efficiency and is a huge driver for formalisation of economy, with particular reference to the Goods and Services Tax (GST) whose complete edifice has been built on digitisation and public schemes like Ayushman Bharat, the biggest health insurance scheme in the world, which is totally paperless, cashless and portable with digitisation as its basis. He further highlighted how Industry 4.0 has captured the imagination of India's industry and entrepreneurs, benefitting the earlier isolated populations by connecting them with the mainstream populations, therefore, opening the

gates of opportunity for many of the disadvantaged in the world. He stressed the significance of technology in assessing various facets of public utilities and delivery services and providing need-based responses like marketing farm products, preparing for extreme weather conditions like droughts and floods, and also to improve education, skill development, law and order situation, build land records and reduce huge impending judicial cases. As such, he emphasised, Digital India is on its way to making digital services a public good where every citizen can have an equal and unrivalled access to it.

While Kant underlined the significance of building on technology and imbibing the benefits of artificial intelligence and blockchain technology, he also cautioned against the pervasive nature of such technology which can be exploited by miscreants and criminals to their own advantage. He further identified the threats of digitisation and social media in terms of influencing elections, creating turmoil in otherwise peaceful societies, inciting violence among societies such as in Sri Lanka and Myanmar, and propagating extremist ideology and online radicalisation. He also highlighted the cyber security breaches in the financial and banking sector.

Kant stated that cyber space being a global common good is transnational in nature, hence, the counter strategy also has to encapsulate all the stakeholders including the government, industry and academia at both the regional and multilateral platforms. He opined that both the citizens and the state are equal partners in the solutions, and have to work together through academia, industry and social group to stitch together strategic response that balances security, and privacy and individual liberties, and does not stifle rights, innovation and creativity. He distinguished between cyber crime and the subsequent responses in military and civilian sphere and called for coordinated action between the two. According to him, the major challenge for India is that the responsibility of handling cyber crimes is diffused across various institutions and agencies, and is grossly inadequate and dysfunctional. Therefore, there is a need for a national data and cyber authority which encompasses a cyber security division, social media division and national police data division cutting across each other which can then manage cyber security hardware gateways and network and in the process manage vital databases and interface with the

public. Not only this, he stressed the importance of early education to inform young minds to use technologies in a useful way. He finally stated on the need to work to create our own models to ensure cyber security.

Keynote Address by Dr. Gulshan Rai, National Cyber Security Coordinator, NSCS, Prime Minister's Office, Government of India

Dr. Gulshan Rai, in his Keynote Address discussed the unique features of the cyber industry distinguishing it from other traditional industries and the opportunities and costs that it entails. He shared the trends in misuse of ICT where 90% was for creating traditional crimes, 9% were the targeted attacks and 1%, which has gained prominence in the last 1.5 years only is the weaponization of ICT like WannaCry, Petya among others. He cautioned that the 1% component of sophisticated crimes is likely to increase in the coming years as the share of traditional crimes (90%) goes down. Dr. Rai identified the peculiar features of the cyber industry makes it challenging to address the problems that it brings.

Firstly, due to free of costs services, there is monetisation of data which is not only limited to ICT companies, internet companies or ISP but has also extended to terror funding and crime funding. Secondly, those who create a product in this industry are not accountable or responsible for the services provided. The third feature of the industry is the service providers claiming to protect the device from the threat due to the unaccountability, and in

disguise collect and monitor data. Consequently, service providers, to detect threats, for instance anti-virus software providers in the barge of defending the device from threat collect the data and monitor activities. He further talked about the paradoxical notion where we live in a world of complexity of cyber space due to the immense benefits and potentials that technologies like AI and ML bring but also the unanticipated impacts, which are not yet comprehended. Though internet was created to strengthen the concept of a Global Village, he noted that the recent patterns have shown a deviation from it.

The issues of privacy, jurisprudence and the legal framework, and the issues of data localisation, ownership and sovereignty are showing a shift away from the notion of open and transparent internet. He further suggested that the policy framework should help strengthen the concept of single cyberspace, and help create a better nation with social prosperity, more wealth and better education.

In the interactive session with the audience, Dr. Gulshan Rai emphasised the need of the government to create a framework where tech-companies should undergo self-regulation and balance the agenda of economic growth and sovereignty. The models for cyber governance should not be isolated, but have a multi-stakeholder approach with shared responsibility.

Session I: Redefining the Rules of Engagement & Knowing the Game Changers

Moderator	Keynote Speakers	Panelists
Syed Munir Khasru Chairman, IPAG	**Richard Wike** Director of Global Attitudes Research Pew Research Centre Washington DC, US	**Ambassador Latha Reddy** Co-Chair of the Global Commission on Stability of Cyberspace, India
	Dr. Stephen Tankel Associate Professor, American University, Adjunct Senior Fellow, Centre for a New American Security, American University	**Dipakshi Mehandru** Senior Advisor Government Affairs & Public Policy Dell Inc.

Wike, in his Keynote Presentation discussed about key findings of a survey done by Pew Research Centre on public opinion about extremism by categorising it into three broad questions:

1. How much support public gives to extremism?
2. Level of concern public have for extremism & its activities?
3. How are concerns about extremism disrupting the politics of nations?

As a response to the first question, Wike stated that public opinion, including those of the Muslim majority countries, was not in much favour of extremism or terrorist organizations. The basis of this finding was a survey done in 2015, where data was collected from large population countries and big majority in these countries had negative view about extremist groups, ranging from 14% in Nigeria to 0% in Lebanon. For the second question, data of 38 countries was surveyed where citizens were asked about the most dangerous international threats facing their countries, where terrorism and extremist groups' activities was a common response by all. The threat of ISIS topped the list of international threat followed by climate change and cyber-attacks respectively. It was in Japan, that cyber-attack topped the list of international threat. As a response to question three it was found that the security-related concerns about terrorism and extremists groups are one factor which the politics of many nations around the globe. He further added that people in Europe think that the influx of refugees would lead to more terror attack in their country.

Dr. Tankel, in his Keynote Presentation, offered key insights on the role of social media and the advantages it provides for online radicalization. He stated that there is no single pathway that leads to radicalisation and discussed the role of online radicalization and encryption technologies in virtual planning as a major challenge to tackling terrorism. He highlighted the advantages that social media provides to propagating extremist ideologies and promoting radicalization, with particular reference to the direct public communication between

individual and terrorist recruiters or facilitators, and the opportunity to engage anonymously. He further argued that pooling with people at social media is much easier and advantageous as compared to traditional websites which generally had password security forums. Social media also provides new ways for sympathizers to be indirectly involved in terrorist activities like providing funds to conduct terrorist operations. These are also known as 'Virtual Terrorism Entrepreneurs' as these are the people who work through social media to enable terrorist activities to create violence. He concluded by making the following three observation:

- There is no single policy fix, public or private for these issues.
- There is tension in combating online radicalization with encryption security (used by terrorists) on one hand and privacy issues on the other hand.
- There is a need of public and private collaboration along with international collaboration for combating online radicalization.

Ambassador Latha Reddy dwelt on the solutions of digital world and its disruptive technologies. According to her, there has to be more international cooperation in internet governance and creation of norms that will govern cyber space. There has to be an enhancement of international peace, security and stability by engaging stakeholders, and proposing norms and policies which would guide state and non-state actors in cyber space. She further pointed out that the recommendations need to be advocated in action and people should ensure that the state and non-state actors do not conduct activities which substantially damage the general availability and integrity of the public core of internet including routing, DNS certification, trust and communication cable. She emphasised the need to develop strong international cooperation norms on the issues of cybercrime and online radicalization among others. She mentioned that the Budapest Convention on cyber-crime and GDPR have been significant development and suggested that new mechanisms like innovation, openness and access need to be incorporated to secure the medium from damages.

Ms. Dipakshi Mehandru discussed about the four pillars of engagement, namely trust, innovation and entrepreneurship, high skill labour force, and sustainable development, through which national, regional and international cooperation could help in increasing the safeguards for the system. She highlighted that internet penetration presently amounted to 24% of the population and it has been anticipated that by 2021, 2 in every 5 people would be connected to Internet. She recommended that the society needs to develop a culture of risk taking for tackling such challenges and also start thinking about the issues of sustainable development now with a future in mind.

Discussion within the Panel

Syed Munir Khasru, the Moderator of the session, observed that the Keynote Presentations point to a trend where there is not much public support for terrorism. On this, he asked the Keynote Speakers, what are the reasons for continuously increasing radical elements and hate speech on online portals and what are the factors that influence people to get involved in such activities. The Panel responded to this by stating that social media platform help build networks, identify groups of people, howsoever small, who support terrorist activities and extremist ideologies and create a global network with multiplier technology. Khasru further asked the Panel to identify the potential positive game changers that could assist the government in securing the cyberspace. Speaking from a policy/public service perspective, Ambassador Latha Reddy suggested the following as the potential positive game changers:

- UN led international coalition of bringing different stakeholders together with different permutation and combination, developing on the model of IAEA.
- Bilateral and regional cooperation initiatives.

Offering the industry perspective, Mehandru identified the following four positive game changers:

- Education by engaging students, teachers and parents.
- Research and development.
- Promoting diversity and inclusion in both public and private sector.
- Democratisation of technology.

Wike suggested that the political elites and the business elites are the two positive game changers that can influence public opinion and contribute to tackling this threat.

Dr. Tankel represented the academia perspective and identified the following positive game changers:

- The experts in the field who could connect technical science with social science to tackle the challenges.
- The strength of academia in cyber space to frame issues and make sense of open source data.

Key Takeaways

- There is a need to identify the ways and processes through which technology has created new platforms for radicalisation, for instance, social media that facilitates communication between the propagators of extremist ideologies and the vulnerable population.
- To address the issue of online radicalization, there is a need to identify the game changers, both positive and negative, in the cyber industry cutting across disciplines and offering holistic perspectives.
- There is a need of public and private collaboration along with international collaboration for combating online radicalization.

Session II: Security & Intelligence Apparatus: Are Old Methods Obsolete? What Paradigm Shifts Are Necessary?

Moderator	Keynote Speakers	Panelists
Maj Gen Alok Deb, SM, VSM (Retd.), Deputy Director General, IDSA	**Farah Pandith** Head of Strategy Institute of Strategic Dialogue, UK	**Benjamin Ang** Senior Fellow, S. Rajaratnam School of International Studies (RSIS), Singapore
	Andrew Balmaks Chairman Institute for Regional Security, Australia	**KPM Das** Cyber Security Trust Officer CISCO India

The Moderator introduced the session and stated that while the radicalising elements had always existed, it is the use of technology for this purpose that has amplified the threat of radicalisation. He pointed out that India emerged as the third most vulnerable risk of cyber threat as per Semantic Analysis of the previous year and suggested that a proper mechanism to counter the cyber threat challenges is needed. He highlighted the use of Force 47 in Vietnam to monitor the internet, and bring down videos and data which are disruptive for country's unity. Further, he emphasised that the nature of cyber space is in itself very secretive and anonymous, and countries getting into cyber space are not likely to share the data. Thus, governments both individually and collectively need to incorporate measures such that cyber threats are curbed.

Pandith, in her Keynote Presentation focussed on the trends in the existing counter-terrorism strategies to address the challenges of online radicalisation and building innovative global programs to counter radical extremism. She identified the following trends:

- Increasing pressure on private sector companies by the government to tackle this issue.
- Existence of multiple identities of extremists who are using online portal making the problem complex.
- The absence of 'other ideas' despite the growing need to saturate market place for ideas with the right kind of many 'other ideas' for the behavioral shifts to happen.

As a response to deal with these trends, she suggested the following:

- To build and design infrastructures and neutral platform to facilitate information sharing.
- Building resilience in a way that is authentic to the community and has more credibility than those spreading radical and extremist ideologies.
- Focus needs to be on the younger generation and reaching out to them.
- Building resilience among children by imparting education of cultural understanding of being a good internet citizen
- Increasing role of civil society organization, majorly at the micro level.

Pandith further discussed the following limitations of the existing resilience mechanism:

- Failure of the countries and existing networks around the world with an understanding about extremism to build this together in a larger way.
- Failure to understand the age at which people get radicalized and then create sophisticated strategies for younger people.

She concluded by stating that a strategy of integrating governments, private sectors and countries all over the world is needed to counter the threat of internet and extremist groups.

Balmaks explored some of the challenges of existing set up of cyber security apparatus and capacity building. He defined radical as a person who has desire for fundamental socio-political change and as a growing community pursue and support far reaching changes in the society which are conflicting and threaten the existing orders. Quoting the advantage of technology, he added that radicals have online existence and technology gives them ease of connection and communication thereby expanding the reach and scale of their operations. He further stated that everyone irrespective of social and economic status, and age have ready access to technology, and social media allows them interaction and participation, and removes technological edge which was once enjoyed by national states. He identified the characteristics of social media, namely the ubiquitous capability, variable purposes, vulnerabilities that allow targeting and manifestation or expression of identity as contribution that facilitate its use as a platform for radicalisation, particularly among youth. Lastly, he dwelt upon the three challenges to existing security apparatus, namely, a radical, a follower and a connector. The strategy to counter this must not be confined to military, police or security forces approach but should include the private sector and communities as well. He suggested that the problem requires an anthropological approach which needs to target the cause by identifying the desire inside the problem.

Ang made the following comments on Balmaks' Keynote presentation:

- Territorial focus, the world totally needs more global cooperation.
- There is too much centralization in looking at the solutions of this problem, more decentralization and flexibility is needed.
- There is easy access to technology, thus government should be able to use technology better. We need to develop norms of technology use.

He further stated that more of social and psychological understanding of the issue is needed along with the technical understanding.

Ang made the following comments on Pandith's Keynote presentation:

- Offline part of building resilience among children is as important as online part. Homes, schools, community should make children understand about the difference between positive narrative that builds up state and negative narrative that builds up violence and destruction.
- The online world does not have accountability and governance and this needs to be changed.
- In creating counter narrative strategies, governments are not the only influential factors.

Das focused on intelligence apparatus to deal with the issue of cyber security and observed identified the following challenges:

- While there is no dearth of ideas for capacity building in the intelligence community at the strategic level, there is a major lack of resources in terms of scale and number of people needed on ground.
- The existing ways of interpreting and filtering of information before sharing in the intelligence team are not appropriate in the light of new paradigm shifts.
- There is a need for new disciplines in the apparatus, particularly from liberal arts who understand how human beings behave. Intelligence community need to look

inward, being more diverse and inclusive, and should develop rich interfaces with the public.

- To manage the encryption of data, there has to be a shift from data to Meta-data where we would require people not only from technical background but rather from other disciplines as well.

Discussion within the Panel

Maj Gen Alok Deb (Retd.) emphasised the basic dilemma of responsibility amongst the stakeholders -government, society, private companies or the individuals; and put the question of taking responsibility at the international level. As a response to this, Ms. Pandith states that all the four entities need to jointly come together and take responsibility of countering this problem. To that Balmaks added that since radicalisation is also an anthropological issue and not necessarily a geographical or national issue, industry is one of the ways through which this issue needs to be looked it. This is because industry is not bound largely by the borders and seeks to break down borders for its own purposes whereas governments may contribute to solidifying those borders when there is actually flow of information through those borders. On the issue of anthropology, Maj Gen Alok Deb (Retd.) discussed about the US program called 'Mapping Human Terrain' in Afghanistan which was started with an aim to understand the population better and enhance cooperation but the program was called off. He thus highlighted that while the objective with such exercises are conducted is noble, understanding the sensitivities of the people and getting them to think in a similar manner is a herculean exercise. Das highlighted the fact that cyber defense and cyber offence are two facets of the same structure. Industry, being the primary market force should permeate this learning to the government. Ang further added to it by stating that each sector is to perform well in their own sector, for instance, while the government has the resources, the private sector has the speed flexibility and understanding of the market.

Key Takeaways

- For building resilience program, more information should be shared amongst all the stakeholders and special focus should be given to children and the younger population. A cultural understanding of being a good internet citizen should be created.
- All the stakeholders should share the responsibility of online radicalization and come together to develop counter narrative strategies.
- A multi-disciplinary model where there is a connect between technical sciences and social sciences, including anthropology and sociology among others needs to be created.
- There is need for global cooperation to develop norms of governance in cyberspace.

Session III: Combating Online Terrorist Propaganda: Role of Major Tech Companies and the Need for a Coordinated Response on Defining the Propaganda

Moderator	Keynote Speakers	Panelists
Shruti Pandalai Associate Fellow, IDSA	**Scott Carpenter** Managing Director, Jigsaw, Google Adjunct Scholar, Washington Institute for Near East Policy New York, US	**Serge Stroobants** Director of Operations Europe and MENA region Institute for Economics & Peace
	Jessie Lowry Francescon Senior Advisor of CVE Communications, US State Department & Director of Dialogue and Communication, Hedayah Centre, Abu Dhabi, UAE	**Kavitha Kunhi Kannan** Public Policy Manager - India, South Asia and Central Asia, Facebook

The Moderator, Pandalai, opened the discussion by her initial remarks on how the misuse of social media has become the bane of digital age. She highlighted that the internet was assumed to bring positive changes like more connectivity and reducing the risk of innovation but it has actually amplified the threat of polarization of ideas making the world more intolerant.

Carpenter, in his Keynote Presentation, focused on Google's institutional practices to counter online radicalization. He highlighted the way that Jigsaw looks at the nexus between online and offline platform and re-enforces each other in effort to keep their users safe. He quoted instances from interview in the Northern Rocky Prison and the findings indicate that there was a moment in time in the funnel of radicalisation where people are making decisions, and there is a small opening to influence such decisions. He then shared that YouTube has 400 hours of video uploaded on Google servers every single minute but the content out there is not found due to their unpopularity. Google then serves ads against them and uses the redirect method to counter the problem. He emphasised that the objective is not to create profound cognitive dissidence but to provide people with what they are looking for and create a cognitive break of small nature. In their 8 weeks of pilot project of people clicking on the ads both in English and Arabic it was found that 320,906 individuals clicked on targeted ads and the click through rate was 79% better than the average click through rate. Lastly, he highlighted the individualistic and localised nature of YouTube and Google searches, making it imperative for the counter narrative strategies to understand the local context for effective implementation.

Francescon, in her Keynote Presentation, highlighted the significance of multi-stakeholder approach in developing the counter narrative strategy. She then discussed how technology has changed the terrorist operations and stated that technology will change the security and military approaches; it will deliver prevention programs via education and job opportunities. It is

going to change international models and initiatives for tackling the terrorism. And it is going to change recruitment efforts. Lastly, the recommendations included, National Action Plans like the World of Communications which is the new frontline in the battle against Violent Extremism (March 2018). Similarly, Global CVE Expo 2019 which is an immersive and interactive space to connect the right people, inspiring cutting-edge ideas and forges new partnerships by bringing those both inside and outside of the CVE community.

Stroobants focussed on the information operation and psychological operation to influence the enemy and re-gain dominance on the battle field facing threat of insurgency and radicalization. He talked about the drivers of terrorist attack and 99.5 percent of them occur to be the existing circumstances. He further highlighted that 90% of the terrorist attacks occur in countries involved in armed conflict, while in the remaining 10%, the majority of attacks occur in countries with high levels of political terror and no respect for human rights. According to him, the main drivers of radicalization are – (a) Justice, (b) Those who advocate justice, and (c) Those who get justice.

After these three steps, recruiters come in and pick up those people who go frustrated with the system and they are the ones who get involved in violent activities. He then concluded by stating that radicalization is a personal process and de-radicalization as a response should also be a personal process.

Kavita Kunhi Kannan talked about the enforcement actions in two ways – (i) how does Facebook employ technology, i.e., Artificial Intelligence (AI) and Machine Learning (ML), and (ii) what human expertise does Facebook has? She mentioned that it has image matching technology where they take lot of symbols, photos and the names of individuals who are connected to terrorist activities across the world and then use AI and ML to trawl across the platform and then bring that content down. Second part to this is language understanding, where certain key words and tags are taken, and put into the AI system which alerts them of the

kind of content they should be watchful about. Once the content is identified, they need to decide that someone is condemning that violence and then take it down. The next part to it is similar to offline terrorist activities, where online terrorist activities are in clusters. So, if the company has taken down the content of specific person who has praised any terrorist activity, the company can actually identify if other friends have similar activity. Regarding human expertise, Kannan highlighted that Facebook has Counter Terrorism (CT) experts, presently over 200 in number who are recruited from various backgrounds like law and enforcement, intelligence or civil society. They together understand the activity and take the content down. Facebook further has about 7000+ content reviewers who look at the content decide whether that is in violation of policy or not and then take it down. What matters is that both AI and content reviewers are able to efficiently take bad content down. Further, she emphasised that radicalisation not only has online stakeholders but offline stakeholders as well. Therefore, counter strategy to address the issue has to go beyond taking the content down and there is a much deeper role to be played by all the stakeholders in the system.

Discussion within the Panel

The Moderator, **Pandalai**, raised the issue of required state resources with Mr. Stroobants, to counter radicalisation with the de-radicalisation strategies. He responded to this by suggesting that the solution to this does not lie in putting people in the prison but rather pulling them through the system in which clinical psychology, anthropology and social science is present to bring them to normal life. Kannan was asked about the ways in which Facebook deals with criticism in cases of non-cooperation with the Intelligence agencies because of their servers being located outside the country or Facebook being banned in the instances of communal content going viral. To this, she responded that internet shut downs have costs and create economic losses for the country, and it is only a temporary solution to the problem, thereby highlighting the need to create permanent solutions to such issues. Another question addressed to Kannan was regarding standard operating procedures to handle crisis especially in India where communal content goes viral, and the existing mechanisms to

deal with this problem. To this, she responded that in India and South Asian, Facebook has established channels with law enforcement agencies for communication and coordination, especially in emergency situations. And secondly, Facebook has to follow a lot of legal processes that are in place. Going through that process may take time but adherence to those legal standards is needed for securing data. The session concluded with the fact that social media should be a force multiplier and national security debate.

Key Takeaways

- The tech-companies can play a significant role in educating and enlightening the citizens against the online radicalization propaganda.
- Major industry players can create innovative counter narrative strategies and work on their actual implementation on ground to combat the threat of online radicalization.
- Understanding the local context and using psychological and behavioral approaches are imperative to for effective counter radicalization strategies.

Session IV: Data Security in Corporations and Financial Institutions: The Menace of Information Theft

Moderator	Keynote Speakers	Panelists
Amit Sharma Additional Director Office of the Scientific Advisor of Defence Minister, DRDO Ministry of Defence, Government of India	**Prof. John Mallery** Research Scientist MIT Computer Science & Artificial Intelligence Laboratory, US	**Omar Sherin** Director of Cyber Security Ernst & Young - MENA Region, Qatar
	Damien Manuel Director Centre for Cyber Security Research & Innovation (CSRI), Deakin University	**Ashish Sonal** CEO, Orkash

Prof. Mallery, in his Keynote Presentation**,** discussed the framework for cyber defence, unfair trade practices, issue of intellectual property theft and other such concerning issues for the financial sector. He discussed about various dimensions of multi-level cyber conflicts and put the financial sector in the critical infrastructure layer of economics. Then he deliberated upon the comprehensive cyber defence framework, including the cyber defense strategy and cyber risk reduction strategy. Both the strategies encompassed several categories such as knowing a threat model, having security and resilience architectures, incentivisation of critical actors, analysing residual risk, creating deterrence architectures and, developing mutual defence alliances and partnerships among others. He dwelt upon the issue of destabilization of the internet trade regime due to economic conflicts and cyber insecurity and highlighted the national flagging of cyber security companies and leading to the fragmentation of ICT component of trade. He deliberated upon important elements of countervailing IP thefts, namely: deterrence by punishment, deterrence by denial, and deterrence by entanglement and discussed about the Multi-Spectrum Adversaries (MSA) who are responsible for cyber insecurity and breaches through remote access of backups, through insiders, supply chain, and leakages. He emphasised on cyber data sharing architecture for rapid threat mitigation and the need of raising information assurance in globalised ICT supply chain. He further suggested the following seven international policy levers for incentivizing better information assurance and resilience:

i) Major vendor unilateral action,
ii) Industry standards for products and services,
iii) Voluntary accords for sectors,
iv) Technology norms,
v) National regulation based on standards,
vi) Policies of supranational entities such as EU and NATO, and
vii) WTO

Prof. Mallery concluded by stating that success in cyber risk reduction requires a comprehensive strategy for cyber defence and solidarity against unfair trade practices is necessary to sustain and modernise the contemporary international trade regime. And finally, the International Vulnerabilities Equities Process (IVEP) can drive phased increases in information assurance in ICT and raises the cost for malicious cyber activity.

Manuel, in his Keynote Presentation, focused on the threats and risk management practices in the banking sector and underlined the challenges of governance in them. He elaborated on the impacts of data breaches on financial sector along with technology implications and concerns. He stressed on four 'W's to consider for cyber security in financial sector -what is important to one's business and asset, the value of data to them, their customers, partners, suppliers and attackers; where the assets are and how they are protected; who is after that asset and why. The motivations, according to Manuel, range from curiosity to political, ideological, financial need and in many cases to gain power. He emphasised that financial organisations should be concerned about cybercrime from the criminal syndicates and trusted insiders, who could be classified into – negligent, ethical and malicious, and also highlighted that the governments around the world are building defensive as well as offensive capabilities to tackle this menace of cyber security breaches.

Manuel further explained the issues of data breaching, GDPR, supplier governance, privacy, and data sovereignty, and the need to be seen from a risk management perspective. He then explained the layers of risk management in the banking sector –(i) the team embedded within the business, (ii) team that provides oversight of that team and rolls up all the detail that has been collected and produced in that business department, and (iii) the order team that monitors and polices within the organisation. He also elaborated on key risk themes from a business perspective which included delivery of services, ability to adapt, fraud and robustness, and security of data.

Sherin highlighted two issues –(i) of malwares being provided as a service that has made the technology breaches easier and, (ii) the issue of attribution in the cyber space. According to him, it is almost impossible to discover who actually had committed the attack especially when the server used for attack was rented and hired by bitcoins. He was of the opinion that there have been discussions on national and policy levels but the problems are more entrenched at the very core of the day to day operations.

Sonal, explained that it is because of the lack of security apparatus at the fundamental level of design of technology that results in vulnerabilities and causes cyber threats. He emphasised that the processes and the systems need to be monitored which include both the normal as well as the abnormal behaviours. Apart from systems' behavior, the human behavior and social engineering should also be taken into consideration while tackling such risks. He mentioned that the financial institutions have 'suspicious activity report' as a very powerful mechanism to deal with cases of abnormal behaviours with the help of open source intelligence. He concluded by emphasising the need to invest more in technologies that are cognitive in nature where data fusion and analytics can be done.

Discussion within the Panel

The panel discussion began with very significant observations by the Moderator, Sharma who raised concern of selling malwares and providing malwares as service -a very prevalent phenomenon that is specifically designed as to not have abnormal behavior and defeat the anti-virus software. To this, Prof. Mallery responded and underscored that classical computer security and design time security is not enough because the adversaries and attackers have multipliers working for them and role of insiders is also a challenge. He further stated that defender's primary objective should be to make multipliers to work for the defender and design security for

monitoring the system to get the behavioural analytics. He added that there is also a question of enterprise and the cost of attacks has to be raised in order to prevent them from happening.

The Moderator then raised the conflicting issues of privacy vs. security vs. usability. In response to that, Sherin stated that when talking about human privacy and human life, the former has to take a backseat and found that the question is not very easy and straightforward to address. He also stressed on 'resilience' because the attackers would eventually find ways to get through the systems and networks despite defence system in place. Thus, the focus should be on recovery and resilience.

Key Takeaways

- Financial sector suffers from technological breaches and cyber threats because of flaws at the fundamental and architectural level of design.
- There is a need for a 'comprehensive framework for cyber defence' in the banking sector.
- As breaches and attacks are inevitable the shift needs to be focused on resilience and recovery. And the cost of attacks has to be raised to avoid cyber threats.
- There is a need to have a comprehensive view while designing security technology with perspectives from businesses, human element, technology, systems, ethics and norms, and law and regulation.

Session V: Data and Policy: Bridging the Knowledge Divide

Moderator	Keynote Speakers	Panelists
Dr. Madan M. Oberoi Special Commissioner of Police (Special Cell and Technology Cell) Delhi Police, India	**Puneet Kukreja** Partner Cyber Advisory and Threat Intelligence, Deloitte, Australia	**Pukhraj Singh** CTO Bhujang, India
	Klon Kitchen Senior Research Fellow Technology, National Security & Science, Heritage Foundation, US	**Rafiqul Islam** Lead Analyst, Cyber Initiative IPAG

Kukreja, in his Keynote Presentation, underlined the significance of viewing data as a key asset. He defined digital transformation as re-engineering operating models, next generation human engagement, quantum computing blockchain ecosystems and artificial intelligence, and emphasised their serious implications. Kukreja further emphasised that breaches are inevitable but what really matters is that people are not subject to extortion and ransomware, their services are not denied and there is no disruption. As it has taken a long time for the policy and law makers to catch up with the pace of innovations, he was of the opinion that the solutions for cyber security cannot be sought at the policy level discussion. He rather suggested that such breaches can only be resolved by individuals as a group as security is a chain of individual decisions and is a shared responsibility. He further stated that data usage should be looked from three perspectives -digital, data and policy perspectives; as these cannot exist in isolation and need to be worked upon holistically. He advocated the shared responsibility model along with a minimum viable controls model on which norms can work on.

Mr. Kitchen, in his Keynote Presentation, highlighted three key trends in the cyberspace – (i) we are innovating faster than we can secure, (ii) the security burden is migrating from the state to the private sector and, (iii) the illusion of "neutrality" is being stripped away. He highlighted that there prevails a kind of techno-idealism which assumes that technology is the key driver of progress, and that economic, social and political bumps and refinements caused by technology should be sparked not avoided. One such unanticipated bump is the shift of security burden to the private sector which was earlier the exclusive domain of the government. Kitchen also underlined the rise of 'digital mercantilism' due to the coercive economic policies followed by certain countries particularly China. The key recommendations made by Kitchen are:

- The government which enjoy exclusive information, capabilities and authority should use it better by sharing it with the industry and acknowledge the presence of other stakeholders in security issues.
- The industry must shed its techno-idealism and adopt a more realistic approach to world affairs by engaging in conversation regarding the geopolitical implications of their technologies and business, and adopt new business practices to anticipate and mitigate significant problems that technologies provoke.
- The civil society can play a significant role in bridging the divide between government and industry through translation and policy innovation.

And finally, he concluded by saying that dialogues among different stakeholders should produce something of value to govt. and to industry, and further stressed on the need of intellectual institutions that are responsible and are able to iterate.

Pukhraj Singh asserted that cyberspace is a contested territory and rather than viewing it as an object of offence and defense, it should be seen in terms of control and non-control because all nation- states try to establish a modicum of control over cyber space. Furthermore, according to him privacy laws such as the General Data Protection Regulation (GDPR) are a defeat since it concedes to the fact of giving up on the agents who consume information and to the agencies that analyse that information. Mr. Singh underlined that there is no difference between observability and identifiability in the cyber space, and control, ownership, and possession of assets in data in cyberspace do not overlap. This is where cyber offence comes into being because it is mathematically impossible to figure who controls the data. On data sovereignty and the possibilities for India, he was of the opinion that India cannot take a middle stand and either has to submit to the hegemonic stand of existing nation-states which control the internet or create a dystopian state which is founded on data sovereignty.

Rafiqul Islam also agreed that the pace of innovation is moving ahead of policy and law-makers and therefore, there is a need to protect and secure different data layers from others as there is no trust in the cyber space. Further, he stressed on the need of having strong law enforcement mechanisms to deal with cases of technology and data breaches.

Discussion within the Panel

The Moderator, **Dr. Oberoi**, initiated the discussion by observing a dichotomy between the physical space, where there is no trust and the regulation is expected from the law enforcement forces, and the cyber world, and an inherent faith in the goodness of people to self-regulate. He questioned whether it is an open admission of insufficiency to be able to enforce our own norms. As a response to this, the issue of 'no trust' in cyberspace was discussed and need for having control mechanisms in place to monitor and report was emphasised. Another guiding question was whether the need for sovereign cyber space is actually about sovereign Balkanized cyber space. Pukhraj Singh responded that notions of territoriality and causality that lead to proportionality, and the dimension of legality fail in cyber. The Panel agreed that demands for data localization and sovereign control would lead to the "Balkanization" of the internet which is not desirable.

Key Takeaways

- Policy makers have not been able to catch up with the pace of innovation. Therefore, strategies to secure cyberspace cannot be solved at the policy level only and need to be done in cooperation with the industry players and other key stakeholders.
- The government and the industry should work together to share information and adopt practices that mitigate the challenges of technology.
- The civil society can play a vital role in bridging the divide between government and industry through translation and policy innovation.
- There is no trust in the cyber space therefore; strong law enforcement mechanisms are required.

Session VI: State Intrusion for Public Safety vs. Citizens' Right to Personal Privacy: Where do We Draw the Line?

Moderator	Keynote Speakers	Panelists
Dr. Sunil Agarwal Deputy Director Cyber Division, National Security Council Secretariat (NSCS), Government of India	**Syed Munir Khasru** Chairman, IPAG	**Albana Shala** Chair IPDC Council UNESCO, France
	Jamil N. Jaffer Adjunct Professor, National Security Institute (NSI); Founder and Director, National Security Law and Policy Program, Antonin Scalia Law School, George Mason University, US	**Munish Sharma** Consultant IDSA

Khasru, in his Keynote Presentation, described the notion of security before and after the internet and elucidated the changes and challenges that the current security regime is witnessing. He highlighted the paradigm shifts in the arena of security with the advent of technology and the dilemma of meeting citizen's rights on one hand and maintaining government accountability on the other. He identified the challenges of balancing citizen's rights and security, majorly as absence of dialogue among state, intelligence and tech companies, and civil entities, and the pace of innovations which has made it difficult for governments to regulate and codify emerging technologies. He further emphasised that the mass surveillance has to be reformed to protect the right to privacy and the citizens' rights to be enshrined in the right to information act. Khasru suggested public policy initiatives for both the intelligence community as well as the government which, among others included, ensuring transparency, accountability and responsibilities towards citizen's privacy, and need for initiatives of greater public outreach programs. He stressed on the need for more consultative dialogues and partnerships among different stakeholders, and more capacity building for policymakers, law enforcers, and data handlers, and finally, the need to modernize the existing surveillance programmes to ensure security and protect privacy.

Jaffer advocated a multi-stakeholder approach on cyber security and stressed on the crucial role that the state, the private actors and civil society as a collective can play in meeting the challenges of cyber threat. He also explicated the cost and benefit analysis in the areas of cyber security and surveillance. According to him, the rapid technological changes, growing IOT and connected smart devices have created a massive increase in quantity, speed, and criticality of data. Jaffer viewed cyber as an element of national power, whereby key actors conduct and deliberate destructive attacks and try to establish long term foothold, and also emphasised on economic costs of such cybercrimes. He further stressed on the need of collective security apparatus that involves the government and the private sector and a common operating picture that empowers private defense and government offence. He emphasised the key

role of civil society in establishing trust and relationship across various divides -consumers, industry and government, to identify the costs and benefits and potential trade-offs and develop methods to rebalance them.

Shala emphasized on the role of the UNESCO as a UN body in terms of the role, the nature and the governance of internet and stressed on the need of global norms and international laws on cyber security. She was of the opinion that all the four pillars of the UN – culture, education, science and communication- put together would contribute to the debate about digital age and the cyber space. She argued that given the debate over data and privacy, continuous dialogue is required among the states, business communities, academia, think tanks and civil society with shared responsibilities.

Sharma, remarked that encryption is the core of privacy. He highlighted how encryption technology is being increasingly used to secure communication channels which terrorists use for launching attacks. He further added that there is no emerging consensus in the international community over the issues of privacy and security which results in different policy frameworks at the national level. He offered four options from a government's point of view, namely; need for developing backdoors; to invest more on resources to have better techniques; to control encryption; and to have strong encryption in place and lawful access to data. He believes that the debate between individual privacy and state security is a zero-sum game, where one will always be compromised to a certain extent for the sake of other.

Discussion within the Panel

Khasru emphasized on bottom-up approach to address the problem and stressed that people need to connect more and touch upon the fundamentals of citizens' protection and state security. Jaffer added to that and stated the fundamental rules have not changed and therefore, the trade-offs between expecting people's protection by the state by giving up on some of the individual rights is essential. The Moderator Dr. Sunil Agarwal highlighted the privacy dilemma of the government where it has to play a dual role to ensure the safety and security of the citizens, and to reconcile it with its role as the guarantor of the right to privacy.

Key Takeaways

- Need for a multi-stakeholder approach and having more consultative dialogues, partnership and collaboration among state, intelligence, business community and civil society.
- Modernize existing surveillance programs to strike a balance between ensuring security and protecting privacy.

Workshops

Workshop by Facebook: Facebook Community Standards Roundtable

On the sidelines of the main conference, Facebook conducted a two-hour workshop on Facebook's Community Standards. The workshop began with the description of Community Standards, which are detailed guidelines outlining what is and is not allowed on Facebook, followed by policies specific to terrorism and hate speech. It was emphasised that Facebook does not allow any organisations or individuals that are engaged in terrorist activities and also removes any praise, support or representation for such groups, leaders or individuals. It was further underlined that Facebook does not allow hate speech because it creates an environment of intimidation and exclusion and in some cases may promote real-world violence. The workshop described the process of framing these policies based on the input from the Facebook community and experts in fields such as terrorism and public safety. The interactive session discussed the significance, role and effectiveness of these policies in combating terrorist activities at the regional and global level.

Workshop by CISCO: Digital Convergence in the Battlefield: A Cyber View

A half-day workshop was conducted for the participants from the Government of India and Ministry of Defence on "Digital Convergence in the Battlefield: A Cyber View". The workshop began with the exposition of the Digital Battlefield and its Components followed by a walk-through of the Security Architectures. Participants were engaged in interactive sessions on Threat Intelligence, emerging propositions for building operational capabilities with a final blueprint on the Security Operations Centres as the foundation for operational outcomes. The workshop drew interesting perspectives and brought together the multiple facets of the cyber components in the battlefield.

Conclusion & The Way Forward

The experts were unanimous in their assessment that while unleashing the human potentials of creativity and ingenuity, the cyberspace also has an inherent risk for threats of unprecedented levels, capable of harming the societal structure at scales never imagined before. There is a strong consensus on the need for a singular cyberspace that is more transparent and better governed while taking care of privacy rights and a more secured environment for adults and children alike. Better coordination among global policymakers and greater collaboration with all stakeholders is essential in pursuit of a singular, undivided cyberspace that can efficiently tackle the threats and propel the human civilization to greater heights of socio-economic development that the internet is supposed to catalyze.

Given the positive outcome of the IDSA-IPAG international conference on cyber security and strong endorsement for continuity in a domain that is in a constant state of evolution, IDSA and IPAG are committed to continue to work together in building on the momentum generated through this event. On that note, the IDSA-IPAG consortium aspires to reach out to all the stakeholders including the policymakers, experts, sponsors, civil society, academicians and media to build on the outcomes of the 2018 conference and organize it again next year, 2019, with a greater setting, broader scope, and at a larger scale.

IPAG

The Institute for Policy, Advocacy, and Governance

info@ipag.org facebook.com/ipag.org @ipag_org www.ipag.org