CYBER 360^0

A SYNERGIA CONCLAVE

Sept 29th-30th, 2015. The Taj West End, Bangalore, India

KEY INSIGHTS

§

SYNERGIA FOUNDATION

Impact Beyond Borders™

CONTEXT

The Synergia Foundation, an interdisciplinary do-tank that primarily focuses on issues related to geo-economics, geo-politics and geo security, has been working for more than a decade to better understand the impact of cyber threats to nation states, business enterprises and civil society. In doing so, we have worked with more than two hundred of the world's best practitioners of security and a number of leading think tanks from around the world. Our research led to the following conclusions:

- Cyber or digital security is an asymmetric threat and it will be hard to equate it with any risk mitigation matrix that has been used before.
- Cyber security should be approached with a 360 degree perspective. It should include international collaboration, external & internal intelligence, web intelligence (WEBINT), human intelligence (HUMINT), open source intelligence (OSINT), signal intelligence (SIGINT), technical intelligence (TECHINT) and supply chain security.
- The current understanding of cybersecurity appears to be more focused on networks. The surface area of networks in threat mitigation is estimated to be between 16-18%.
- Organizations should identity what are the key assets that they would need to protect.
- There is a definite cost arbitrage in mitigating such threats.
- Cyber threats should be handled at a board level / top management and not be considered as a technology problem.
- Top management of companies must be equipped with insights and leading edge practices to make informed decisions about cyber security.

METHODOLOGY

Cyber 360 is the outcome of two years of intense research by the Synergia Foundation on both the traditional and non-traditional aspects of cybersecurity. All the topics and panel discussions were aligned to the research outcomes. The primary objective of Cyber 360 was to bring together some of the brightest practitioners of security and policy to debate on the various topics. Over the span of two days, Cyber 360 brought together key stakeholders from the government, industry, strategic thinkers, media and civil society on a single platform to analyze the current approach towards network security and attempt to create a more holistic security framework to build resilience against cyber threats.

A range of key note presentations, panel discussions and interventions from the participants who were selectively invited, provided a distinct opportunity to ideate and learn from leading cyber security experts, strategic thinkers, law enforcement agencies, government and media from all over the world.
Cyber 360 was also able to highlight commercial opportunities that exists for technology companies in the cyber domain.

Below are the insights drawn from each of the sessions of the conference.

KEYNOTE ADDRESS

DAY ONE

Dr. Arvind Gupta
Deputy National Security Advisor,
Government of India

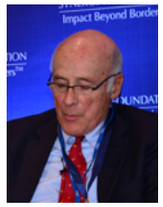
- Cyber diplomacy is a new arm of any country's diplomatic endeavors. The concern of countries today is maintaining a balance between national security and human rights in the sphere of ICT, and how to deal with threats in cyberspace to political, social and economic systems. Cyber issues affect the prosperity and security of nations and has become an important element of foreign policy.
- IN applying existing law in cyberspace issues, the focus is on state norms of behavior, confidence building measures, information exchange, capacity building and cooperation.
- If international law applies to cyberspace, then a state would have inherent right of self-defense. There is as yet no international consensus on the basic definitions including what is cyberspace, what a cyber-attack is and what does cyber security mean.
- The scale and breadth of Digital India provides unprecedented business opportunities to Indian companies. There is increasing need for a synergy between the governments and other stakeholders to evolve a suitable security policy framework and technical eco-system to make Digital India a success.
- Technology is far ahead of law, law enforcement and policy making when it comes to the internet. This calls for complex and innovative approaches.

DAY TWO

G.K. Pillai
Former Home Secretary,
Government of India

- There has been an exponential growth of cyberspace and internet technology. This also points to the question as to why vulnerabilities were not corrected previously. Are vested interests involved?
- Over the years, hacking is only going increase as large sums of money are involved. State-supported actors in this field will also increase.
- A consensus on the global commons is unlikely as every country wants to look after its own national and economic interests.
- Ongoing dialogues like the Global Commission on Internet Governance (GCIG) are important to obtain some amount of cooperation in cyberspace. Cooperation will exist only when nations feel that the issue will threaten their national interests.
- Going forward, it is important to practice basic cyber hygiene in-order to remain protected from attacks.

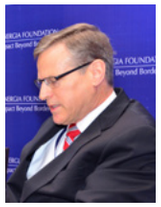
KEY INSIGHTS



The New World Order

Joseph S. Nye
Former Dean, Kennedy School at Harvard University
Carl Bildt
Former Swedish Prime Minister
Shivshankar Menon
Former National Security Advisor, India

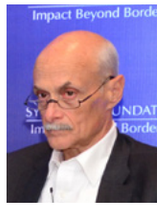
- Power transition from one government to another is not what should be discussed, but power diffusion from the state to non-state actors. This diffusion is leading to new sets of issues that are transnational and no one government can control it.
- Entropy, the inability to get work done, is a far greater threat. Focus should be on how to deal with diffusion of power and ensure the population do not suffer from entropy.
- Cyber space is a domain where technology empowers the insurgent, the individual, the weaker party, or the small group by giving them communications reach and access to data and other people's systems. Cyber, today, has only given a fresh lease of life to the existing order. It has added another weapon to the arsenal that states, small groups and individuals deploy.
- Cyber has the potential to amplify and disrupt the global order. The imminent question, therefore, is whether past learnings can help create a new cyber order?



Cyber 9/11

Dr. Patrick Cronin
Director – Centre for New American Security (CNAS)
Shivshankar Menon
Former National Security Advisor, India
Praveen Swami
National Editor (Strategic and International Affairs), The Indian Express

- There is a need to enact policies with countries in order to raise the belief in reliability of data. Non-state actors have gained much more cyber capabilities than governments.
- There is a widening gap between what is technically possible and what is socially acceptable.
- Terrorists have not yet attacked critical infrastructure yet as it does not have the coercive effect of cutting someone's head off. State and Non-state actors find it valuable to disrupt such technology. However, in the future, terrorists may attack such infrastructure.
- Therefore there is an urgent need to secure the environment to ensure that the common man retains a sense of security and trust in the government.


Cybersecurity: A 360^{O} Perspective

Dr. V.K. Saraswat
Former Chief of DRDO
Michael Chertoff
Former United States Secretary of Homeland Security
R.K.Radhakrishnan
Sr. Dy. Editor, Frontline

- Security cannot be an afterthought.
- Enterprises and countries need to identify what is their key asset and what is the system in place to protect it.
- Segmenting key assets is better as few will have access to the most important asset in the organization.
- Recognize methods to monitor network, acquire technology and skilled personnel to ensure continuity of protection.
- It is also important to have a resilience strategy in place, as the difference between a bad experience and catastrophe is time.
- While sharing of information is important, it is also important to gather data from open source intelligence and behavioral algorithm, which will provide an early warning and minimize the impact.



Resetting Intelligence: A New Approach

Melissa Hathaway
Led the Comprehensive National Cybersecurity Initiative for President Barack Obama & Former President George Bush
David Omand
Former Director of GCHQ
Prabha Rao
Additional Secretary, Cabinet Secretariat, Govt. of India

- Consider terrorist activities like businesses. They have HR capabilities, a strategy to expand markets and to finance their operations.
- Digital intelligence is important in this fight against terrorism. The volume of communications globally is so huge and growing that it is easy for the criminal or terrorist to hide.
- Sharing of information is needed to better understand the pattern of data exchange as technology is providing faster means of communication.
- Bulk data analysis has helped intelligence agencies to thwart terrorist attacks.
- Mining any digital data that relates to individuals has to be conducted throughout with respect for the privacy rights of the individual, and with proper legal authority.
- Security and Privacy are not alternatives. Both are important and can be obtained with the help of the 3Rs: rule of law, regulation and oversight and restraint in their use, so that these powerful digital tools – and the use of more traditional human agents and informers – are at all times governed by the principles of legality, necessity and proportionality.
- As we are competitor to a business we do not like (terrorist activities), it is important to obtain new tools and processes to disrupt their flow of goods and services.

Cybersecurity: The Board Dilemma

Bruce McConnell
Senior Vice-President, EastWest Institute
Avinash Vashistha
Former Chairman & Country Managing Director, India, Accenture
Ajay Nanavati
Former Managing Director, 3M India

Raviraj Rao
Head, Security Services Sales & Solutioning at Enterprise Security Risk Management, TCS

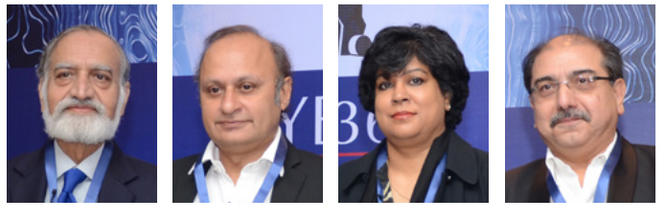
- Analyze the risks of the company and classify them as high impact, mid-range and low impact risks.
- Five key questions to help Board members understand cybersecurity are:
  - What key information or technology needs to be protected? Protecting everything means protecting nothing.
  - What are the risks against which the organization/information/technology should be protected?
  - How are the risks prioritized?
  - What are techniques required to mitigate these risks?
  - What are the residual risks and how will they be managed?
- Cybersecurity can be categorized as securing confidentiality, integrity and availability of the information.
- Businesses need to understand that cybersecurity is like any other business risk and need to involve Board members, as CIOs alone cannot identify the risks.
- While IT can be a business enabler, it has exponential potential to be a disabler too. Hence it is important to gather intelligence from open source to be prepared, and thereby mitigate the risks.
- Integration of three R's - risk assessment, readiness and response is important to counter cyber threats.
- While corporates do a reasonable job of assessment, they lack in readiness as it entails investment and thus the robustness of the response suffers.
- Regular review of cybersecurity risks need to be done.
- There is a need to prioritize the risk from a criticality perspective rather than trying to address everything. Maximize the protection against the highest priority cyber-threats and thereby minimize the risk to the enterprise.

Counter-terrorism and Countering Violent Extremism

Hormis Tharakan
Former Chief of the Research and Analysis Wing, India
Sultan Al Qassemi
Commentator on Arab Affairs
M.N. Reddi
DGP, Home Guards, Fire & Emergency Services and Civil Defence, Karnataka

Ambassador Dian Triansyah Djani
Ministry of Foreign Affairs, Indonesia

- Violent extremism is caused by conflict in ideologies, culture and so on. Handling extremism need not be technical alone, it needs Human Intelligence (HUMINT) too.
- Social media is no longer an open space for activists to express themselves freely and without inhibitions. There is online policing being done to monitor content. Online hackers affiliated to or supportive of governments across the region, such as the Syrian Electronic Army, launched denial of service attacks on certain accounts while pro-government workers intimidated activists using the same social media platforms that activists had previously employed.
- The once liberal and secular activist-dominated social media landscape has made way for conservative clerics or extremist groups.
- Content has to be delivered carefully. It requires global cooperation to effectively counter malicious content.
- The target market for extremist ideology is 25-30 year olds as youth are more susceptible to new ideas due to ignorance and lack of education.
- The rise of sectarian issues are due to corruption, unemployment, graft, marginalization of youth. This makes it a fertile ground to spread extremist ideologies.
- It is important to tackle real-life issues that are leading to extremism, like corruption, unemployment, militarization of the Middle-East and spread of propaganda through religious leaders.
- Radicalization of Islamic youth in India is real though in small numbers. Cyberspace has enabled terror to become borderless.
- While it is important to spread the good message via conventional mediums (role models, sports and movies), it is equally important to hire youth who are tech-savvy to counter the spread of such ideology through effective use of technology.



Re-Imagining Media in the Age of Cyber

Kiran Karnik
Chairman, CII National Committee on Telecom and Broadband
Uday Singh
Managing Director at Motion Picture Association
Neena Gopal
Resident Editor, Deccan Chronicle
Biren Ghose
Country Head, Technicolor, India

- A big change in the traditional media is in creating, curating and selecting content. Today content is created by citizens – if it's interesting it goes viral. This has a negative impact as malicious reports and content can adversely affect businesses.

- In the consumer space the set top box is going to be the key place to protect data. There will be 50 billion connected devices across the planet over the next three years. So the possibility of threats multiplying dramatically remains strong.

- Economic contribution to the economy is approximately 50,000 crores, creating 1.8 million jobs. Digital technology is a boon and a bane. A boon because it gives a tremendous opportunity to repurpose, create content in new ways and reach new, very specific audiences.

- While piracy is big problem, another problem is that a lot of the content lies on servers that are outside India's domain – so how do we tackle the issues that come up with jurisdiction?

- High risk advertising is exposing young children to gambling, pornography, malware, psychotropic drugs. These are serious crime syndicates at work. This can be fixed when our laws and enforcement becomes coordinated to bring about respect for copyright and IP.

- Site blocking is a solution– technologies exists to show details of the piracy, which allows fingerprinting, watermarking. However the solution requires cooperation with the servers outside as well. Legislative processes have to be made which can make content protection practically possible.

Building Cyber Capacity: Role of Industries

Rajendra Pawar
Chairman, NIIT
Bruce McConnell
Senior VP, EastWest Institute
Kinshuk De
Head Business Operations, Enterprise Security Risk Management, TCS

- There is a need to incentivize the space of cybersecurity. The space providing IT products and services will be worth 120 billion dollars in 2017 - which translates to a huge opportunity for India which could have approximately 20 billion dollars in the area of services.

- In human capacity field, expertise and perspective building could happen if the people in cyber could switch back and forth from government to industry sector– this is happening in the US and also in other countries now. Cooperation and information sharing between governments and companies is crucial.

- IT industry will be 350 billion dollars as an industry by 2025, NASSCOM recommends that cybersecurity industry share should increase from 1% to 10%. Another recommendation is that the size of the cybersecurity industry in India should be targeted at 35 billion dollars, creating 1 billion new jobs and 1000 startups in cybersecurity.

- In order to capitalize on this growth, there is a need for industry development, technology development, skill development and policy development.

KEY INSIGHTS



Digital Security

Dr. Paul Twomey
Former CEO & President of ICANN
Nandkumar Saravade
CEO, Data Security Council of India
Kamlesh Bajaj
Founder CEO at Data Security Council of India

- The cost of cybersecurity is around 20 trillion dollars, however the benefits of securing the organization from cyberattacks will be 108 trillion dollars.
- It is necessary to look at the value of the organization from the adversary's perspective.
- The success of a campaign like Digital India depends on security.
- It requires capacity building, delivering authenticated services to a growing base of internet users, protecting the rights of the individual, and having an incidence response strategy in place.
- Combination of self-regulation, compliance, and market forces will make Digital India a success.



Threats to Critical Infrastructure

Melissa Hathaway
Led the Comprehensive National Cybersecurity Initiative for President Barack Obama
& Former President George Bush
Sachin Burman
Director, NCIIPC
Latha Reddy
Former Deputy NSA, India

- Internet based services are embedded in every aspect of infrastructure from agriculture to services.
- The primary infrastructure that needs maximum protection are – Energy, Telecomm and Financial systems. These infrastructure needs to be declared off-limits even during wartime.
- It is necessary to clean up infected infrastructure, share actionable information and have better products.
- There should be a coordinated center to report a problem and disseminate effective information to others. It is important to look at cybersecurity holistically and not as an IT problem.
- In the absence of secure devices it is necessary to have cybersecurity experts to create a secure environment.



Smart Cities: How Secure?

Gopal Rathnam
Chief Information Officer, CISCO
T.T. Thomas
Former Chief of Technology,
National Intelligence Grid (NATGRID), India
T.M. Veeraraghav
Resident Editor, The Hindu

- The amount of resources that are required to be invested in cyber security are humungous – how will this be justified to a population that is untouched by the cyber- world.
- Benefit of a smart city is to deliver the most efficient citizen service possible. However, connectivity is not ubiquitous. So the notion has to be implemented in smaller communities first, and then become part of the larger picture.
- There is a need for centralized command centers, data centers to handle emergencies and disasters.
- There is no silver bullet – it is an integrated, holistic approach starting with citizens who have to use social media, centralized helplines, technologically equipped beat cops, people who can analyze problems real time and create solutions.
- A smart city will have a collection of interdependent services. We have so far not got the opportunity to test resilience, vulnerability across services that are so disparate.
- Investments towards this, which the government has in mind, may not address the sophistication to actually run and model a well-functioning smart city.
- Key in cybersecurity is to handle it from an architectural standpoint – which would mean it should be policy driven – and policies have to be embedded at the infrastructure level.



Dark Web and Crypto Currency

Dr. M.M. Oberoi
Director, Cyber Innovation, Interpol
Pindar Wong
Chairman and President VeriFi Limited
Prabha Rao
Additional Secretary, Cabinet Secretariat, Govt. of India

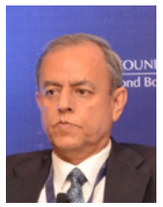
- The global trend today shows that there has been an increase in random cases, attacks are shifting to mobile platforms and that crime is being provided as a service.
- Content in the Dark Web is not searchable and hence organizations like Interpol are trying to index websites in the dark web. These kind of technology can enable a 'lone wolf' kind of terrorist attack.
- Cryptocurrency (Bitcoin) is emerging as a medium of online transactions in the dark net for physical crimes. For instance, hacking an email will cost 0.451 bitcoin while hacking a website will cost 1.1 bitcoin.
- Bitcoins are attractive as it can be transferred anywhere without digital copies.
- There is no counterfeiting due to the block-chain technology, has higher processing power, and has proper tracking record.
- Can this technology be used to empower law enforcement agencies?



Internet Architecture as a Proxy for State Power

Dr. Laura DeNardis
Professor, School of Communication,
American University, Washington
Anriette Esterhuysen
Executive Director of the Association for Progressive Communications (APC)
Gordon Smith
Former Canadian Deputy Foreign Minister and NATO Ambassador

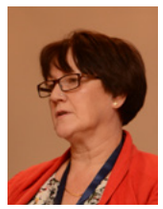
- The internet architecture is being tampered with by the governments and military for security purposes.
- Weakening public encryption of data for security purposes only increases security vulnerabilities in the internet governance.
- Internet freedom is no longer merely about content. Fundamental human rights depend upon an underlying system of technological infrastructure that creates the conditions for innovation and civil liberties online.
- A significant shift in policymaking has been the introduction of laws - regulating where private companies store data and how infrastructure is physically configured. “Holding” data in a fixed location is incompatible with engineering principles like reducing latency, load balancing, and basic traffic engineering. It is also incommensurable with business models predicated upon global customer bases and workforces.
- Encryption backdoors, data localization, and DNS alterations are examples of government interest in altering the design of Internet infrastructure to achieve policy objectives. They all raise questions about the implications of these alterations for the stability and security of the Internet itself; for civil liberties; and for the pace of innovation online.


Hybrid Warfare

Lt. General Davinder Kumar
Veteran, Indian Army
Lt. General Prakash Katoch
Veteran, Indian Army
Col. K.P.M. Das
Veteran, Indian Army

- The exploitation of the under-privileged have led to violence for resolving territorial disputes, oppose religious beliefs, restore perceived economic balance etc.
- The reaction of the weak/poor against the rich/ strong through technological asymmetry is called hybrid warfare.
- Today we have an enhanced digital battlefield, where multiple domains can be attacked simultaneously and at the speed of light.
- Conflicts are increasingly no-contact, remotely controlled, collusive, partly outsourced and often involves non-combatants in active roles. This has been aided by emerging trends in technologies, and rests on some recent disruptions in the areas of open technologies and standards, massively parallel computing, big data and deep analytics, social media adoption and Internet of Things.
- Net-centricity among opponents has been enabled by the trends in machine-to-machine learning and connects, automating many layers of control in the battlefield.
- Technologies will equip the military leaders, but with an immense range of options, the winner will be the one who is able to package it together with the correct doctrine. Operational discipline and relentless execution will stay as determinants of battle outcomes.

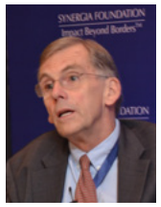



Cyber & Space

Dr. K.D. Nayak
Director-General, DRDO
Dr. Patricia Lewis
Research Director,
International Security at Chatham House

- Low Intensity conflicts are already going on in cyberspace testing the strength of each nation.
- Vulnerability of satellites to cyber-attacks is important to every citizen. Cyber-attacks on satellites can spread to other areas – to ground stations, other connecting technologies. Some of the satellites being put into orbit are cyber insecure – particularly those in the civilian and research sector. This causes a problem because all technologies are linked – one weak link could cause a great damage.
- Ways to attack a satellite: Jamming, spoofing, harnessing/taking remote control of a satellite, knock out a satellite by frying the solar panels. One of the big issues identified is frequency hopping.
- There is a need to pay particular attention to the ground stations which are perhaps the most vulnerable. There is a need to build more resilience into navigational data systems.
- It is important to have co-operation between the IT security systems and space security; and to connect governmental experts and academics of both sectors. Industries need to take responsibility for their satellites, and their security. Industry sharing approach necessary – like in the banking and energy sectors.

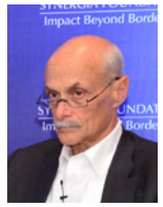
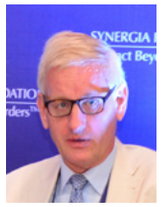
DINNER TALKS




Securing the State

David Omand
Former Director of GCHQ,
Praveen Swami
National Editor (Strategic and International Affairs),
The Indian Express.

- Modern intelligence requires intelligence about people, rather than about traditional targets such as armed forces and state organizations.
- Terrorism is used also as a tool to attain political aspirations.
- Policing, in order to create a secure state, requires new patterns of cooperation between intelligence and law enforcement, and between both of them and private industry and commerce, that is so often the target of hostile attack.
- There is also an urgent need to ensure capacity building so that the police, army, bureaucracy, government and private sectors are well-equipped to handle security issues.
- It is essential to understand the power of cyber diplomacy. Multi-stakeholder governance model of internet can defeat the fragmentation of internet and ensure that it cannot be used as a vehicle for internal censorship and political repression.
- The causes of conflict in the 21st century will not be so different from those of previous centuries since they are rooted in the human condition; the way they are expressed will differ. However which of these 21st century struggles becomes serious armed conflicts, erupting into violence by open warfare, insurgency, or terrorism, is as hard to predict today as it was in the past. Therefore Securing the State is never going to be easy.

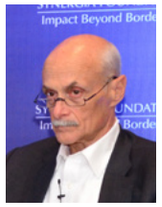




Security in the 21st Century

Michael Chertoff
Former United States Secretary of Homeland Security
Carl Bildt
Former Swedish Prime Minister
Vikram Sood
Former Chief of RAW

- In 2010, despite 9/11 and Iraq conflict, the world looked quite optimistic. Five years later, however, the outlook is much different.
- Terrorists are always one step ahead of counter-terrorism activities. This is even more magnified with the use of cyber space for malicious activities.
- There is a need to build capacity to counter such threats.
- Some of the trends seen in the past years are:
  - Rise of global disorder: The idea of jihadist extremism has now metastasized. Power vacuum has magnified problems as seen in Libya and Syria. Problems in one area today has ripple effects in other parts too.
  - There is an erosion of generally accepted principles of war. This is seen in Russian invasions and China's expansionist regime.
  - Developments in Cyber is causing much alarm among nations. There has been theft of Intellectual Property which can affect economies, and destructive attacks on critical infrastructure. This calls for the need to build security in IoTs.
- Western democracy today is seriously challenged, with the rise of theocratic and other models of governance.
- There is a need for strategic assessment on how to deal with disorders and the pressure on borders.

PRE-CONFERENCE: KEY INSIGHTS



Conference on Digital Security: Investing in a Secure Supply Chain

Michael Chertoff
Former United States Secretary of Homeland Security
Dr. Paul Twomey
Former CEO & President of ICANN
Tobby Simon
President, Synergia Foundation

- Each player in the supply chain is of equal importance. Any compromise at any stage of the supply chain can jeopardize the entire enterprise and its operations.
- Managing cyber security is a large part of the of risk management narrative. Policies and the architecture in relation to security, should be in place before any enterprise focuses on the tools and the people who handle them.
- Structure of all enterprises' cyber design tends to be the crafted in a similar manner, making it easier for hackers to intrude into the company's servers and files.
- In the fields of outsourcing and software, there are going to be far higher security requirements in place than ever before.
- Cybersecurity being compromised is a human problem – it happens through negligence, or wilfully. There can never be total safety against cyber attacks – you can only limit the time of attack and keep increasing resilience. Identify the most precious assets and protect them.
- Comprehensive approach is necessary – with human and technical aspects. Identify the problem area, move fast to resolve the issue - this is what helps to build resilience and minimize loss.
- The weakest link and the smallest companies are targeted over the larger ones.
- Companies who follow the larger IT companies' model of going to great lengths to always be better than average in their cybersecurity measures, are the ones who have a greater advantage. They always want to partner with those who can ensure least risk.
- Enterprises and their CIO's end up looking at cyber related tensions through very limiting lenses; a broadened perspective is required and should not be limited to that of networking. Achieving resilience is becoming an existential challenge – and requires a different approach to the executives who are taking the decisions. The IT professional may not be the best candidate to ensure supply chain resilience and safety.
- Enhancing of cyber security is in sync with the larger Indian narrative set by the Government of India to digitalise the economy and to make smart cities. These initiatives require a healthy and a strong foundation.
- Architectural security of IoT is required to ensure a secure our digital environment. Digital India campaign, "Make in India" initiative and Smart cities project will fail to achieve any success without Digital Security.

POST-CONFERENCE: KEY INSIGHTS




Cyber Security and Space Security: High Level Expert Roundtable

Tobby Simon
President, Synergia Foundation
A.S. Kiran Kumar
Chairman, ISRO
Dr. Patricia Lewis
Research Director, International Security at Chatham House
Dr. K.D. Nayak
Director-General, DRDO

- Cyber-security today, is inherently linked with satellite management and space security.
- Cyber space and real space started with the purpose of providing services to the people, in an accessible, sustainable manner. The security of these services is only now coming to the forefront in discussions.
- The threats to cyber space can affect the economics of countries and can also encourage terrorism.
- Military satellites have always been protected with the available technological facilities. The problem exponentially increases when the military starts using the civilian systems for military purposes to reduce their budget.
- India has been a leader in building satellites at cheaper prices for the masses to experience the benefits of satellite technology. If we start building protected satellites and have defense mechanisms in existing commercial/ civilian satellites then the production costs will go up. This will affect the market of the satellites.
- Terrorist organizations tend to hide sensitive data in plain sight. They transmit sensitive data through open source mediums of information pool on the World Wide Web. This helps camouflage sensitive data within a larger pool of similar data which makes it difficult to find.

GOING FORWARD

The proceedings of the conference will be sent out in the form of a detailed report to all the participants. In the following months, each of the sessions at Cyber 360 will be taken up individually to provide a deeper understanding into the subjects. This will be done in the form of focus group workshops or webinars comprising twenty of the best practitioners in the world.

SYNERGIA CONCLAVE 2016

With over four hundred years of combined experience in strategic security, the Synergia Foundation works on real time primary information to pursue high quality, non-partisan research and draws on a global network of resources to offer the most comprehensive analysis and impactful solutions. The Synergia Conclave is designed to be an annual event of the Synergia Foundation. The purpose of the conclave is to study complex issues that pose existential or cause systemic threats which would affect human security; to make practical interventions within the existing scenario, and the industries that use it; and to ensure that solutions are well designed and implemented within industry, government and policy making processes.

If you are interested in collaborating with Synergia Foundation on the next Synergia Conclave, on any of the above areas, or to study a problem and suggest interventions that requires interdisciplinary learning, please contact:

Ann / Sambratha
Embassy Diamante, 34, Vittal Mallya Road,
Bangalore 560 001, India.
Tel: + 91 80 41971000 Fax: +91 80 41971001
Email: ann@synergiagroup.in / sambratha@synergiagroup.in

SYNERGIA FOUNDATION

Impact Beyond Borders™