सत्यमेव जयते

BPRD

आ नो भद्राः क्रतवो यन्तु विश्वतः

Indian Cyber Crime Coordination Centre

Proceedings

National Level Webinar on

Cyber Security

Preparedness for next 10 years

(25th November, 2021)

National Cyber Crime Research & Innovation Centre (NCR&IC)

BUREAU OF POLICE RESEARCH AND DEVELOPMENT

Ministry of Home Affairs, Government of India

Promoting Good Practices & Standards

Proceedings

National Level Webinar on

Cyber Security

Preparedness for next 10 years

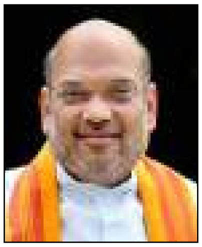
(25th November, 2021)

National Cyber Crime Research & Innovation Centre (NCR&IC)
BUREAU OF POLICE RESEARCH AND DEVELOPMENT
Ministry of Home Affairs, Government of India

अमित शाह

सत्यमेव जयते

गृह मंत्री एवं सहकारिता मंत्री
भारत सरकार



संदेश

भारत के संविधान की सातवीं अनुसूची के अनुसार **'पुलिस'** और **'लोक व्यवस्था'** राज्य के विषय हैं। राज्य / केंद्र शासित प्रदेश कानून के प्रावधानों के अनुसार अपनी कानून प्रवर्तन एजेंसियों के माध्यम से साइबर अपराध की रोकथाम, उनका पता लगाने, जांच और अभियोजन के प्रति प्राथमिक रूप से उत्तरदायी हैं। इसके अलावा, राज्य/केंद्र शासित प्रदेश साइबर अपराध, फौरेंसिक आदि के क्षेत्र में चुनौतियों का सामना करने के लिए पुलिस कर्मियों को प्रशिक्षण देकर अपने साइबर सुरक्षा तंत्र/बुनियादी ढांचे को मजबूत करने और अपनी कानून प्रवर्तन एजेंसियों की क्षमता निर्माण के लिए जिम्मेदार हैं। राज्य सरकारों की विभिन्न योजनाओं के अंतर्गत क्षमता निर्माण के लिए उठाए गए कदमों के लिए केंद्र सरकार परामर्शों और वित्तीय सहायता के माध्यम से मदद करती है।

सरकार ने साइबर अपराध से निपटने के लिए कई पहल और योजनाएं शुरू की हैं। भारतीय साइबर अपराध समन्वय केन्द्र, 14C योजना ने राष्ट्रीय साइबर अपराध रिर्पोटिंग पोर्टल (www.cybercrime.gov.in) लॉन्च किया है, ताकि जनता महिलाओं और बच्चों के विरूद्ध साइबर अपराधों पर विशेष ध्यान देने के साथ-साथ सभी प्रकार के साइबर अपराधों से संबंधित घटनाओं की रिपोर्ट कर सकें। ऑनलाइन साइबर संबंधित शिकायतों को दर्ज करने में सहायता प्राप्त करने के लिए एक टोल फ्री नम्बर:- 1930 शुरू किया गया है।

राष्ट्रीय साइबर अपराध अनुसंधान और नवाचार केन्द्र (NCR&IC) कानून प्रवर्तन एजेंसियों के लिए अनुसंधान आधारित समाधान विकसित करने हेतु विभिन्न हितधारकों की क्षमताओं का लाभ उठाने के लिए बीपीआरएंडडी मुख्यालय, नई दिल्ली में स्थापित 14C का एक महत्वपूर्ण कार्यक्षेत्र है। मुझे खुशी है कि वे उभरती हुई साइबर सुरक्षा चुनौतियों से संबंधित विभिन्न महत्वपूर्ण विषयों पर नियमित रूप से वेबिनार भी आयोजित करते हैं।

देश के नागरिकों के लिए साइबर डोमेन सुरक्षित करने के लिए NCR&IC और BPR&D द्वारा किए जा रहे कार्यों के लिए मैं अपनी शुभकामनाएं प्रेषित करता हूँ।

(अमित शाह)

नित्यानन्द राय
NITYANAND RAI

सत्यमेव जयते

आज़ादी का अमृत महोत्सव

गृह राज्य मंत्री
भारत सरकार
नार्थ ब्लाक, नई दिल्ली – 110001

MINISTER OF STATE FOR
HOME AFFAIRS
GOVERNMENT OF INDIA
NORTH BLOCK,
NEW DELHI - 110001

संदेश

मुझे खुशी है कि बीपीआरएंडडी मुख्यालय, नई दिल्ली में स्थापित राष्ट्रीय साइबर अपराध अनुसंधान एवं नवाचार केंद्र (NCR&IC) कानून प्रवर्तन एजेंसियों के लिए क्षमता निर्माण तथा साइबर अपराध से निपटने हेतु, अनुसंधान एवं विकास समाधान विकसित करने के क्षेत्र में कई गतिविधियों का नेतृत्व कर रहा है।

केंद्र सरकार ने साइबर अपराधों के प्रति जागरूकता फैलाने के लिए चेतावनी/परामर्श जारी किए हैं तथा कानून प्रवर्तन कर्मियों/अभियोजकों/न्यायिक अधिकारियों की क्षमता निर्माण में वृद्धि सहित साइबर फोरेंसिक सुविधाओं में सुधार आदि महत्वपूर्ण कदम उठाए हैं।

भारतीय साइबर अपराध समन्वय केंद्र (14C) की स्थापना के माध्यम से सरकार ने व्यापक और समन्वित तरीके से साइबर अपराधों से निपटने के लिए कानून प्रवर्तन एजेंसियों को एक फ्रेमवर्क और ईकोसिस्टम प्रदान किया है।

जैसा कि साइबर अपराधों का परिदृश्य तेजी से बदल रहा है, अनुसंधान संस्थानों के लिए कानून प्रवर्तन एजेंसियों को समय पर जानकारी देना महत्वपूर्ण हो जाता है। मुझे उम्मीद है कि साइबर अपराध जांच एवं डिजिटल फोरेंसिक के आवश्यक ज्ञान के प्रसार से संबंधित महत्वपूर्ण विषयों पर यह वेबिनार कानून प्रवर्तन एजेंसियों के ईकोसिस्टम के लिए क्षमता निर्माण पहल को बढ़ाने का एक अच्छा तरीका है।

"आगामी 10 वर्षों के लिए साइबर सुरक्षा तैयारी" विषय पर वेबिनार आयोजित करने के लिए मैं बीपीआरएंडडी की पूरी टीम को बधाई देता हूं।

(नित्यानन्द राय)

नई दिल्ली।
18 फरवरी, 2022

Office Tel.: 011-23092870, 23092595, FAX No. : 011-23094896

अजय भल्ला, भा.प्र.से.
AJAY BHALLA, IAS

सत्यमेव जयते

आज़ादी का अमृत महोत्सव

गृह सचिव
Home Secretary
भारत सरकार
Government of India
नार्थ ब्लाक / North Block
नई दिल्ली / New Delhi

MESSAGE

I would like to congratulate the entire team of the National Cyber Crime Research and Innovation Centre, NCR&IC, and the enabling leadership of the Bureau of Police Research and Development for conducting regular webinars on very crucial subjects with regard to cyber crime prevention and investigation.

2. The Ministry of Home Affairs, Government of India, has set up the Indian Cyber Crime Coordination Centre, 14C, under which seven distinct verticals are working towards providing crucial leads like providing cyber threat intelligence, research based solutions for cyber crime investigation, cyber crime reporting and capacity building of law enforcement agencies to augment their fight against cyber crimes.

3. The theme of the Webinar, "Cyber Security Preparedness for Next 10 Years", clearly indicates that the NCR&IC is working with a long term perspective to fulfill its mandate in a professional manner. I urge the law enforcement agencies to make use of the expertise of the NCR&IC and equip themselves with cutting edge technological abilities to respond to the menace of cyber crime.

1/3/22

(Ajay Bhalla)

Place : New Delhi
Dated : 01.03.2022

बालाजी श्रीवास्तव, भा.पु.से.
महानिदेशक

Balaji Srivastava, IPS
Director General

Tel. : 91-11-26781312 (O)
Fax : 91-11-26781315
Email : dg@bprd.nic.in

पुलिस अनुसंधान एवम् विकास ब्यूरो
गृह मंत्रालय, भारत सरकार
राष्ट्रीय राजमार्ग-8, महिपालपुर,
नई दिल्ली-110037

Bureau of Police Research & Development
Ministry of Home Affairs, Govt. of India
National Highway-8, Mahipalpur,
New Delhi-110037

MESSAGE

The setting up of the National Cyber Crime Research & Innovation Centre (NCR&IC) at the BPR&D Hqrs. and its branch, the National Cyber Crime Research, Innovation and Capacity Building, at the CDTI, Hyderabad, has been a major technological milestone in the Cyber Research and Training capabilities of the BPR&D. The NCR&IC, as part of the umbrella scheme of the Indian Cyber Crime Coordination Centre (14C), MHA, has been striving continuously to strengthen and augment the capacity of Law Enforcement Agencies (LEAs) in thier efforts of Cyber Crime prevention and investigation.

NCR&IC has come up with a plan of hosting a regular series of webinars on different emerging topics and subjects related to Cyber space. In this sequence, the 3rd webinar on the theme “Cyber Security Preparedness for Next 10 Years” was organised on 25th Nov 2021 at BPRD HQs, New Delhi. More than 170 participants from all States/UTs, CAPFs and CPOs attended.

This webinar is a result of the sincere efforts of Sh. Karuna Sagar, IPS, IG/Director, Modernization, Brig. Navrattan Joshi, PSO (Electronics), Dr. M M Gosal, SSO (T&T) and Cyber Security Researchers at the NCR&IC, BPR&D. I record my appreciation for their hard work.

I am sanguine that the proceedings of this webinar will be very useful for our Police Forces. These should go a long way in stimulating a new dimension in documenting a decadal road map for Cyber Security Preparedness towards Cyber Crime Prevention and Investigation.

Balaji

(Balaji Srivastava)

“Promoting Good Practices and Standards”

नीरज सिन्हा, भा.पु.से.
अपर महानिदेशक

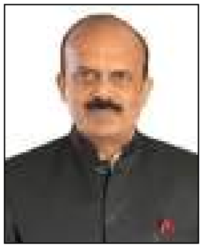
Neeraj Sinha, IPS
Additional Director General

Tel.: + 91 11 26781341 • Fax: 91 11 26782201
Email: adg@bprd.nic.in • Website: www.bprd.nic.in

सत्यमेव जयते

पुलिस अनुसंधान एवम् विकास ब्यूरो
गृह मंत्रालय, भारत सरकार
राष्ट्रीय राजमार्ग-8, महिपालपुर,
नई दिल्ली-110037

Bureau of Police Research & Development
Ministry of Home Affairs, Govt. of India
National Highway-8, Mahipalpur,
New Delhi-110037



MESSAGE

In a world that is changing fast, we would do well to sometimes pause and reflect. And look ahead. In our lifetime in recent memory, cyberspace has transformed so dramatically, that the early memories of its slow and uncertain technology, have faded. The power and vigor of the internet in transforming the way we live our lives is for all to see. As with all things good, cyberspace, however as the designated custodians for nurturing and preserving the safety and security of the ambient environment, the police and security agencies of the country have a central role. With technology advancing by leaps and bounce, the capability of inimical forces to target internet based applications has risen dramatically. Apart from the threat from such individuals and cyber criminals, there also remains the issue of target attacks by enemy countries.

In the backdrop of the emerging environment of potential threat to vital interests of the nation as well as security concerns of individuals and commercial groups, issues of cyber security have come to occupy center stage. Engaging with issues of cyber security and conducting an audit of preparedness, remains an absolute imperative.

I would like to compliment Dr. Karuna Sagar, Director Mod Division of the Bureau, and his entire team, particularly Brig. Navrattan Joshi, PSO (E), Dr. Manjunath M Gosal, SSO (T) and Cyber Security Researchers at the National Cyber Research & Innovation Centre (NCR&IC) for publishing the proceedings of a webinar styled 'Cyber Security Preparedness for Next 10 Years', conducted on November 25, 2021. The idea is to dissemination of the deliberations of the webinar to the larger police and security fraternity.

(Neeraj Sinha)

"Promoting Good Practices and Standards"

डॉ. करूणा सागर, भा.पु.से.
महानिरिक्षक / निदेशक (आधुनिकीकरण)

Dr. Karuna Sagar, IPS
Inspector General/Director (Modernisation)

Tel. : 91-11-26782023
91-11-26782030 (F)
Email : igmod@bprd.nic.in

पुलिस अनुसंधान एवम् विकास ब्यूरो
गृह मंत्रालय, भारत सरकार
राष्ट्रीय राजमार्ग-8, महिपालपुर,
नई दिल्ली-110037

Bureau of Police Research & Development
Ministry of Home Affairs, Govt. of India
National Highway-8, Mahipalpur,
New Delhi-110037

EXECUTIVE SUMMARY

Government of India has rolled out an umbrella Scheme "Indian Cyber Crime Coordination Centre (14C)" to combat cyber crime in the country, in a coordinated and effective manner. The scheme has seven components. National Cyber Crime Research and Innovation Centre (NCR&IC) is one of the seven verticals under the Indian Cyber Crime Coordination Centre (14C) which was allotted to the Bureau of Police Research and Development (BPR&D) with the aim of detecting various types of Cyber Crime and preventing them.

Realizing the fact of ever increasing cases of Cyber Crimes and the need to evolve effective strategies for prevention and investigation of crimes taking place in cyber space, NCR&IC organized a National level Webinar on "Cyber Security Preparedness for Next 10 Years" from 11 AM to 1:15 PM on November 25, 2021 at the BPR&D Headquarters, New Delhi. More than 170 Police Officials from CAPFs, CPOs and Other Police Forces from States/UTs attended the webinar.

The webinar was addressed by eminent subject matter experts coming from three verticals of Cyber Security R&D endeavors viz. Academia, Industry and Law Enforcement Agencies. This way, the webinar offered a rich insight to Law Enforcement Officers on the Cyber Security Preparedness from three different perspectives.

Sh. Neeraj Sinha, ADG, BPR&D opened the meeting with his welcome address wherein he emphasized on the importance of understating the new challenges cyber space is throwing before law enforcement agencies and gave examples that how the Cyber Warfare has evolved in a manner in which one can wreak havoc into the land of adversaries without even dirtying his/her hands.

Sh. Balaji Srivastava, DG, BPR&D delivered his inaugural address. He informed the participants that NCR&IC is one of the seven verticals of Indian Cyber Crime Coordination Centre (14C)

Scheme. Due to rapidly evolving technology the threat landscape is changing continuously. Artificial Intelligence (AI), Machine Learning (ML), Internet of Things (IoT), Cloud Technologies and the rise of cryptocurrency have increased the challenges for investigators. Therefore, it is our responsibility to upskill ourselves and keep ourselves abreast of every latest progress taking place in the cyber world.

Sh. Venkatesh Murthy K, Director, Data Security Council of India, delivered his talk on "Digital Forensics: why the Police should care about it'. He discussed about the Privacy and Police in a Digital Forensic context. He also mentioned about the time consuming factors in the digital forensic process and proposed solutions for speeding up the same. He pointed out the admissibility of the digital forensic evidence in the court of law and challenges associated with it.

Dr. Manan Suri, Associate Professor, Electrical Engineering, IIT Delhi, delivered his talk on 'Implication of Hardware and Artificial Intelligence (AI)'. He gave a brief introduction about a research group viz. Non Volatile Memory and Neuromorphic Research Group is working along with CYRAN AI Solutions at IIT Delhi. While dealing with the hardware aspect of Cyber Security Dr. Suri went on explaining how semiconductor devices are vital in powering the entire digital world. Internet of Thing (IoT), Smart Cities Beyond 5G, Social Media, Healthcare/Genomics, Government Works, Defense, Security & Space, Retail & Finance and Industry 4.0.

Dr. Balsing Rajput, Ph.D., DCP, Technology and Crime Prevention, Mumbai Police, delivered his talk on 'Cyber Security Preparedness for next 10 years: LEA Perspective'. During the talk he discussed about today's Cyberspace Scenario, Law Enforcement Perspective, technologies shaping the next decade, emerging Cyber Threat Landscape, Cyber Security Preparedness areas and way forward for LEAs.

The officials participating in the webinar had got a good opportunity to learn and upgrade their knowledge in Cyber Security Preparedness for next decade. They actively took part in Q&A sessions followed by each talk and enriched their awareness. Overall, it was an interactive and informative webinar about various perspectives for prevention and investigation of new age Cyber Crimes.

(Karuna Sagar)

CONTENTS

1 **Webinar Agenda** **2**

2 **Proceedings** **3**

3 - Session – 1 5

4 - Session – 2 14

5 - Session – 3 27

6 **Contact List of BPR&D officers** **34**

7 **References** **35**

Webinar AGENDA

Webinar Theme:
Cyber Security Preparedness for next 10 years

Mode of Webinar: Online (Cisco WebEx)

Objective of Webinar: To provide an interactive session for Law Enforcement Agencies on emerging cybercrimes, new techniques and methodologies for investigation, prevention and modern-day challenges.

Time	Sessions
11:00AM-11:05AM	Welcome Address - ADG, BPR&D
11:05AM-11:10AM	Inaugural Address - DG, BPR&D
11:10AM-11:40AM	*Session 1:* **Sh. Venkatesh Murthy K,** Director, Data Security Council of India ***Topic – Digital Forensics - Why the police should care about it !***
11:40AM-11:50AM	*Q&A - Session 1*
11:50AM-12:20PM	*Session 2:* **Dr. Manan Suri,** Associate Professor, IIT Delhi **Topic – Implications of hardware for the future of cyber security**
12:20PM-12:30PM	*Q&A - Session 2*
12:30PM-01:00PM	*Session 3:* **Dr. Balsing Rajput, IPS** DCP, Mumbai Police **Topic – Cyber security preparedness: LEA's perspective**
01:00PM-01:10PM	*Q&A - Session 3*
01:10PM-01:15PM	Vote of Thanks - IG (Mod)

PROCEEDINGS

National Cybercrime Research and Innovation Center (NCR&IC) is a vertical of Indian Cybercrime Coordination Center, MHA and is situated at Bureau of Police Research & Development, New Delhi.

In order to provide a platform where LEAs from across the country can learn about emerging cyber security and cyber crime challenges from top cyber security experts, NCR&IC has decided to organise a series of monthly webinars.

The third webinar on the theme ”Cyber Security Preparedness for Next 10 Years” was organised on 25th Nov 2021 at BPRD HQs, New Delhi through WebEx. More than 170 participants from All States/UTs, CAPFs and CPOs attended the webinar.

Following are three esteemed speakers one each from LEAs, industry and academia who delivered their talk:

1. **Sh. Venkatesh Murthy K,**
   Director, Data Security Council of India

2. **Dr. Manan Suri,**
   Associate Professor, IIT Delhi

3. **Dr. Balsing Rajput, IPS**
   DCP, Mumbai Police

Dr. Karuna Sagar, IG/Director (Mod), BPR&D welcomed Sh. Balaji Srivastava, DG, BPR&D, Sh. Neeraj Sinha, ADG, BPR&D at the event.

ADG, BPR&D delivered his welcome address by welcoming all the participant and the distinguished speakers. He expressed his compliments to the NCR&IC team, Modernisation Division and DIG (Mod) for organizing webinar on important topics of cyber security and cyber crime. He informed that as the rapid advancement and development are taking place in cyberspace so are the adversaries upgrading their modus operandi in committing cybercrimes. He emphasized on the importance of understanding the new challenges cyber space is throwing before law enforcement agencies and gave examples that how the cyber warfare has evolved in a manner in which one can wreak havoc into the land of adversaries without even dirtying his/her hands. ADG, BPR&D urged all the participants to learn the new ideas and wisdom from the distinguished speakers present in the webinar.

Sh. Balaji Srivastava, DG, BPR&D delivered his inaugural address.

He informed the participants that NCR&IC is one of the seven verticals of Indian Cyber Crime Coordination Center (I4C) Scheme and it has got three mandates and they are as follows:

a. Identify cyber security challenges and provide research based solutions

b. Work for the capacity building of LEAs

c. To disseminate knowledge and experiences of LEAs and other stakeholders in the area of cyber security

He mentioned that in order to provide the advanced technological solutions to LEAs to augment their fight against cyber crime, NCR&IC has initiated several R&D projects in partnership with the country's premier research institutions. These ongoing projects are expected to provide research based solutions employing cutting edge technology for LEAs.

He said that due to rapidly evolving technology the threat landscape is changing continuously. Artificial Intelligence (AI), Machine Learning (ML), Internet of Things (IoT), Cloud Technologies and the rise of cryptocurrency have increased the challenges for investigators. Therefore, it is our responsibility to upskill ourselves and keep ourselves abreast of every latest progress taking place in the cyber world.

While explaining the objective of the webinar he said that the theme of todays' webinar is "Cyber Security Preparedness for Next 10 years". The objective of the Webinar is to provide an interactive session for Law Enforcement Agencies on emerging cyber crimes, new techniques and methodologies for investigation, prevention and modern-day challenges.

DG, BPR&D urged the participants of the webinar to actively interact with BPR&D to utilize the potential of NCR&IC and even render useful feedback to further align their functioning to meet the requirements of LEA's.

Brig. Navrattan Joshi, Principal Scientific Officer, BPR&D and Dr. Sarabjit Kaur, NCR&IC Professional moderated the programme.

Session 1

Topic: Digital Forensics Why the police should care about it

Venkatesh Murthy K (Director)
Data Security Council of India, India

Mr. Venkatesh Murthy discussed Privacy and police in a digital forensic context.

- Reasonable expectation of privacy
- Data that may not be relevant to the case may be perused by police during the course of investigation
- Focussed queries while analysing digital media
- Satisfy OECD principles: OECD principles:
- Collection limitation, Data quality, Purpose specification, Use limitation, Security safeguards, Openness, Individual participation and Accountability

He suggested few points for the investigation officers as follows:

- Should not perform a significant number of additional tasks that would invade the privacy of a third party.
- Limit data related to parties who are not under investigation.
- Record accidental and intention accesses of private data that is not relevant to the investigation

He discussed about the time consuming factors in the digital forensic process.

Can courts give warrant to inspect only a certain portion of the Hard Disk ?? Even if the police know specific information about the files they seek, the data may be :

- Encrypted,
- Mis-labelled,
- Stored in hidden directories, or
- Deleted - unallocated

Nowadays, IP address based investigation is a challenging task. It is very difficult to identify the culprit behind the crime scene.

He also discussed about the limitation of forensic such as:

- Live acquisition of hard disk- there would be changes in the hard disk by the time acquisition is completed
- Is a phone acquisition forensically sound ? NO
- Two different acquisitions of same cell phone - Acquisitions don't match
- A cell phone when switched ON, changes its state instantaneously

Then, he pointed out the admissibility of the digital forensic evidence in the court of law as per his discussion evidence should be Lawfully collected, Relevant to the case Authentic and reliable. In case of encrypted hard disk Imaging the hard drive would result in a forensic copy of the encrypted data. Powering off the computer with whole disk encryption will make it useless

He briefly mentioned about the new data sources such as:

- IP-based closed-circuit televisions (CCTVs)
- Internet of Things (IoT) devices (e.g., temperature sensors),
- Autonomous vehicles,
- Data on cloud- OneDrive, Dropbox, Egnyte
- Self-hosted cloud storage

He also raised an important issue pertaining to data wiping technology which causes the data disruption. Investigation officers must be careful at the crime scene. Don't Pull the plug of the computer system otherwise:

- Encryption programs, pulling the plug may result in having nothing to examine.
- Trojan horse defense
- Loss of exculpatory evidence

Evidence is dynamic in nature and the suspect may result in Introduction of an Error. Suspect knows how to hide by:

- Disrupt forensic techniques by using counter methods
- Errors can also be introduced during the examination and interpretation of digital evidence. for example, misreading 03:13 A.M. as 3:13 P.M., results in the wrong records being retrieved, implicating the wrong individual.

Knowledge and expertise in handling the evidence determine the evidence quality and importance in court, which affects the jurors' decision. If any procedure was conducted incorrectly, then the evidence might become inadmissible in court. The Challenge in the digital forensic domain is : forensic tools are cost & availability.

Tools have an important role in the forensic investigation process. But, Digital Forensics isn't about just using tools. An investigator is expected to have a deep understanding of the underlying technology he/ she is dealing with.

Followings are the Types of Digital Forensics tools:

- Proprietary
- Open Source
- Free
- YOUR OWN

He mentioned that, Investigator must have a Sterile hard disk for creating a forensic copy and avoid using the same HDD for different cases.

He has discussed about following Digital Forensics concern areas the Law enforcement agencies must be focused on:

- Case handling
- Investigatory budgets
- Staffing
- Training and education
- Lab setup and tool availability
- Analysis procedures
- Interpretation of results
- Reporting

He then discussed the ISO for the digital forensic domain. Guidelines for Identification, collection, acquisition and preservation of digital evidence ISO 27037. Government should focus on Strategy to build DF capability in LEA.

In case of Survey/triage forensic inspection, Targeted review of all available media to determine which items contain the most useful evidence and require additional processing.

- Preliminary forensic examination: Forensic examination of items identified during survey/ triage as containing the most useful evidence, with the goal of quickly providing investigators with information that will aid them in conducting interviews and developing leads.

- In-depth forensic examination: Comprehensive forensic examination of items that require more extensive investigation to gain a more complete understanding of the offense and address specific questions.

He suggested that, there are many resources for the LEA'S pertaining to digital forensic investigation so the cyber forensic practitioner can learn the new technology such as

International Organization on Computer Evidence- I.O.C.E

- Created in 1995
- Act as a forum to collaborate and exchange information about Cybercrimes and Digital Forensics.
- Attributes:
  - » Consistency with all legal systems.
  - » Allowance for the use of a common language
  - » Ability to instill confidence in the integrity of evidence

G8 High-Tech Crime Subcommittee

- Formed in 1997 by G8 states (France, Germany, Italy, the UK, Japan, the US, Canada, & Russia).
- Goal: " to ensure that law enforcement agencies can quickly respond to serious cyber-threats and incidents".
- Document: Principles on Transborder Access to stored Computer Data-Data Principles on Accessing Data stored in a foreign state.
- Preservation of stored data in a computer system
- Expedited Mutual Legal Assistance
- Transborder access to stored data not requiring legal assistance

NEW!! Subscribe to our new meeting announcement email distro under the Subscribe menu link!

Scientific Working Group on Digital Evidence

The **Scientific Working Group on Digital Evidence (SWGDE)** brings together organizations actively engaged in the field of digital and multimedia evidence to foster communication and cooperation as well as to ensure quality and consistency within the forensic community.

SWGDE - Scientific Working Group on Digital Evidence

- Started in 1998.
- The SWGDE works as the US-based representation for IOCE efforts.
- SWGDE is composed of members from: Government, Legal community, Private industry, and academia

The International Association of Computer Investigative Specialists- IACIS

- Started in 1989
- Non-profit, volunteer organization wholly dedicated to training, certifying and providing membership services to computer forensic professionals around the world.
- The IACIS Certification Program consists of : • BCFE • WFE • MDF
- Digital Investigation Process methods • Mark Pollitt • U.S. Department of Justice • Palmer • Carrier and spafford
- Education, Training, and Awareness • General Awareness • Basic Training • Formal Education • Professional Certifications and Accreditations • Specializations

He mentioned that, government should more focus on the Education, Training, and Awareness at user level, they have suggested the training schema as below:

- General Awareness
- Basic Training
- Formal Education

- Professional Certifications and Accreditations
- Specializations

Educational Roadmap pertaining to Technical Knowledge for LEA's as mentioned below:

- Introductory
- Investigation principles
- Evidence management
- Computer systems basics
- Operating systems
- File systems
- Networking protocols

Further, he suggested many domains for basic level intermediate levels and advanced level.

Topics for Intermediate levels as follows:

- Cryptography
- Mobile devices
- Incident response
- Cloud & network forensics

Topics for advance levels as follows:

- Systems development- knowledge about the systems development lifecycle (SDLC) etc.
- Security architecture- to know how and where the implementation of administrative, technical, and physical security control can create greater capabilities for digital forensics

Apart from the technical training he also pointed on the non technical training for doing the work efficiently at the workplace such as:

- Time management
- Analytical skill
- Technical writing
- Communication skills
- Critical thinking
- Interrogation skills
- Interpersonal skills
- Leadership

- Project management
- Conflict resolution
- Budget management
- Resource management
- Strategic mindset

NSDC (National skill development corporation) also offers the certification course for the forensic practitioner which is known as “Forensic specialist”.

Apart from that, forensic practitioners also should enroll in the vendor specific certificate to enhance and enrich their forensic skill set and these are paid certificates, such as:

- Encase Certified Examiner
- Paraben Certified Examiner
- Access Data Certified Examiner

He suggested the vendor neutral certificate for the digital forensic practitioner in the LEA’s, such as:

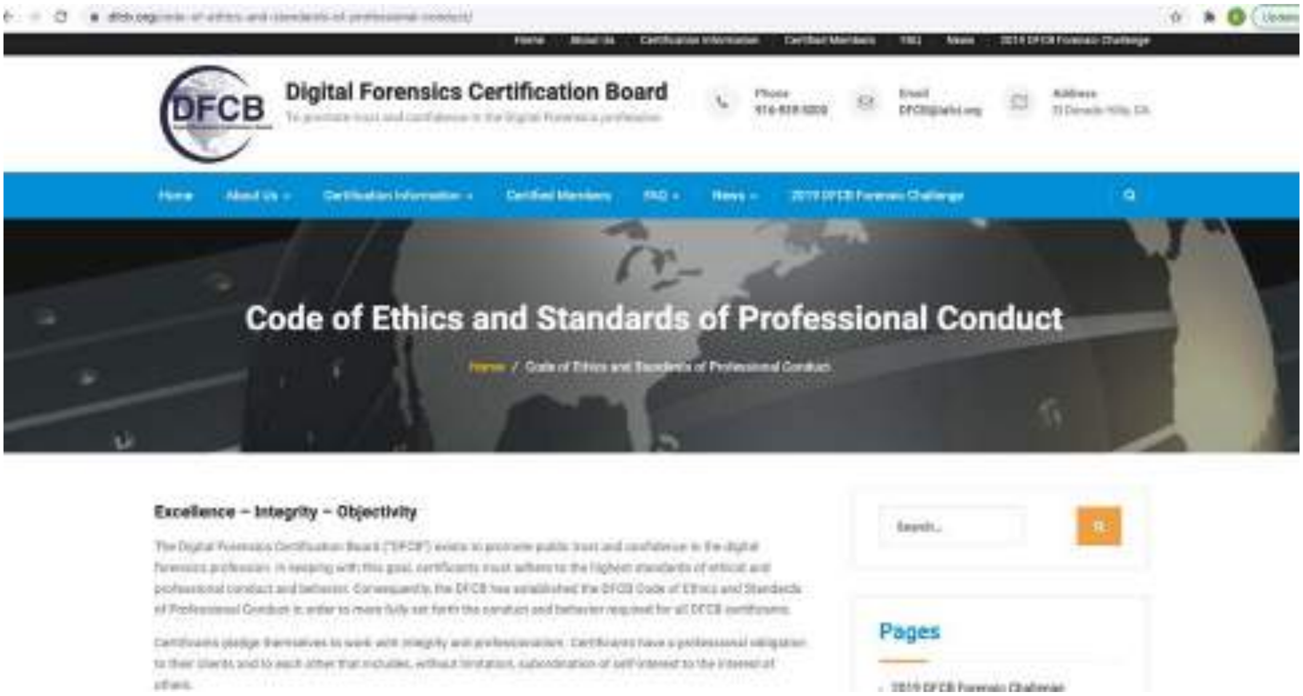
- SANS- GIAC
- IACIS
- Access data Certified Examiner
- High Tech Crime Network

During the talk, he also suggested that many Conferences, Blogs, Forums, Podcasts are there for Forensic practitioners and they must participate for knowledge sharing and knowledge enhancement.

He enlightened on topics related to ethics & professional conduct that are important for the forensic practitioner.

- Fact-1: Digital forensic practitioners possess specialized and unique knowledge which if not governed properly, have the potential for misuse.
- Fact-2: Your team may encounter a situation that puts them in a difficult position, challenging their ethics and conduct.

Create an approach to Recognize, Classify & Manage the issues within boundaries and obligations as a professional. He suggested international ethics and conduct for the same.


Home
About Us
Certification Information
Certified Members
FAQ
News
2019 DFCB Forensic Challenge
DFCB
Digital Forensics Certification Board
To promote trust and confidence in the digital forensics profession
Phone
Email
Address
Home / Code of Ethics and Standards of Professional Conduct
Search...
Pages
2019 DFCB Forensic Challenge

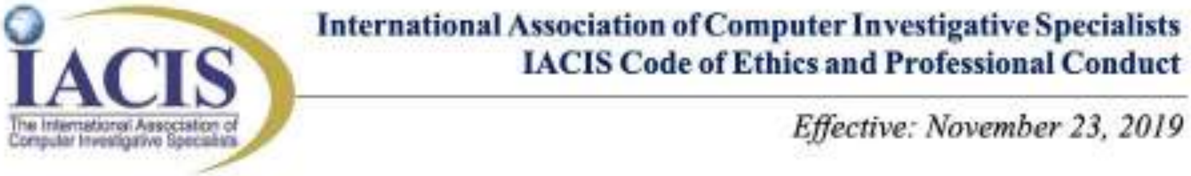
Code of Ethics and Standards of Professional Conduct

Excellence – Integrity – Objectivity

The Digital Forensics Certification Board ("DFCB") exists to promote public trust and confidence in the digital forensics profession. In keeping with this goal, certificants must adhere to the highest standards of ethical and professional conduct and behavior. Consequently, the DFCB has established the DFCB Code of Ethics and Standards of Professional Conduct in order to more fully set forth the conduct and behavior required for all DFCB certificants.

Certificants pledge themselves to work with integrity and professionalism. Certificants have a professional obligation to their clients, and to each other that includes, without limitation, subordination of self-interest to the interest of others.

Ethics in Digital Forensics- IACIS


IACIS
The International Association of Computer Investigative Specialists

International Association of Computer Investigative Specialists
IACIS Code of Ethics and Professional Conduct

Effective: November 23, 2019

Ethics in Digital Forensics- ISFCE

ISFCE · International Society of Forensic Computer Examiners ·

The International Society of Forensic Computer Examiners®

Code of Ethics and Professional Responsibility

Mr. Venkatesh Murthy's talk ended with a brief session of open Q&A.

Reference:

- https://www.iacis.com/training/basic-computer-forensics-examiner/
- http://www.digitalrecordsforensics.org/drf_links.cfm?cat=org
- https://www.swgde.org/home
- Digital Forensics and Investigations by Jason Sachowski, CRC Press
- https://onlinelibrary.wiley.com/doi/epdf/10.1002/spy2.123

Session 2

Topic: Implications of Hardware and Artificial Intelligence (AI)

Dr Manan Suri
Associate Professor, Electrical Engineering, IIT Delhi

Dr. Suri started his discussion on the given topic under following outline/aspect:

l Brief Introduction

l Aspect 1: Cyber Security Implications from Hardware Side

l Aspect 2: Cyber Security Implications from AI Side

He gave a brief introduction about a research group viz. Nov Volatile Memory and Neuromorphic Research Group is working along with CYRAN AI Solutions at IIT Delhi.

Research group was formed in 2014 and subsequently the CYRAN startup was founded in 2018 with a strength of 25+ researchers.

CYRAN stands for Cyber Raksha + Artificial Intellignce (AI) + Nanoelectronics.

CYRAN works under following areas:

1. Cyber - Physical Security Hardware Solutions
   a) Hardware Crypto Primitives
   b) Storage Security
   c) Hardware Forensics
2. AI Hardware-Software Edge Solutions
   a) Authentic/Biometric - AI
   b) Geo AI

c) Industry 4.0 AI

d) Educational Technology (EdTech) AI

While dealing with the hardware aspect of cyber security Dr Suri went on explaining how semiconductor devices are vital in powering the entire digital world. Internet of Things (IoT), Smart Cities Beyond 5G, Social Media, Healthcare/Genomics, Government works, Defence, Security & Space, Retail & Finance and Industry 4.0.

Since the hardware aspect is the common vulnerability threat in the entire cyber world, Cyber security has got coupled to cyber physical security in the modern age.

For the next 10 years following areas will be of critical concern:

l Security (Cyber/Physical)

l Beyond 5G Communication

l Artificial Intelligence and Analytics

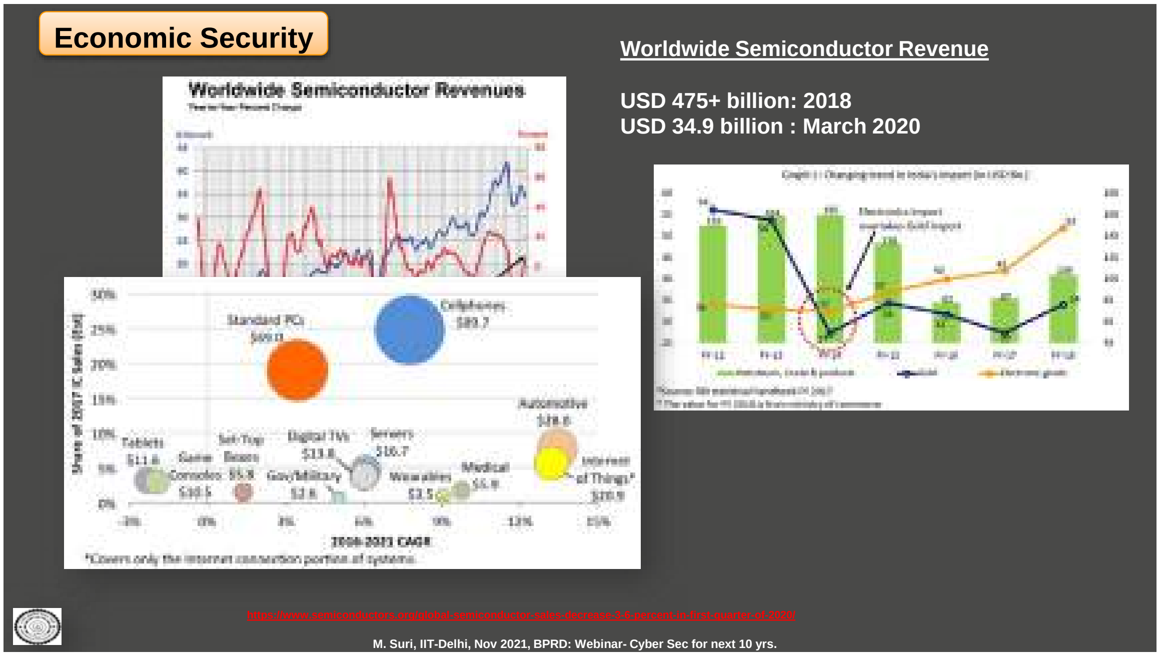
l Sustainability and Smart Cities

l Quantum Computing, post-quantum crypto

l Healthcare sector

Dr. Suri emphasized on the importance of hardware in cyber security by saying that "we are fooling ourselves if we believe that we can do any meaningful security in the above areas without paying attention to semiconductor/hardware".

While discussing the commerce of the hardware industry, Dr. Suri showed Ministry of Commerce data which indicates that 2014 onwards India imports more electronic goods than gold.



Economic Security

Worldwide Semiconductor Revenue

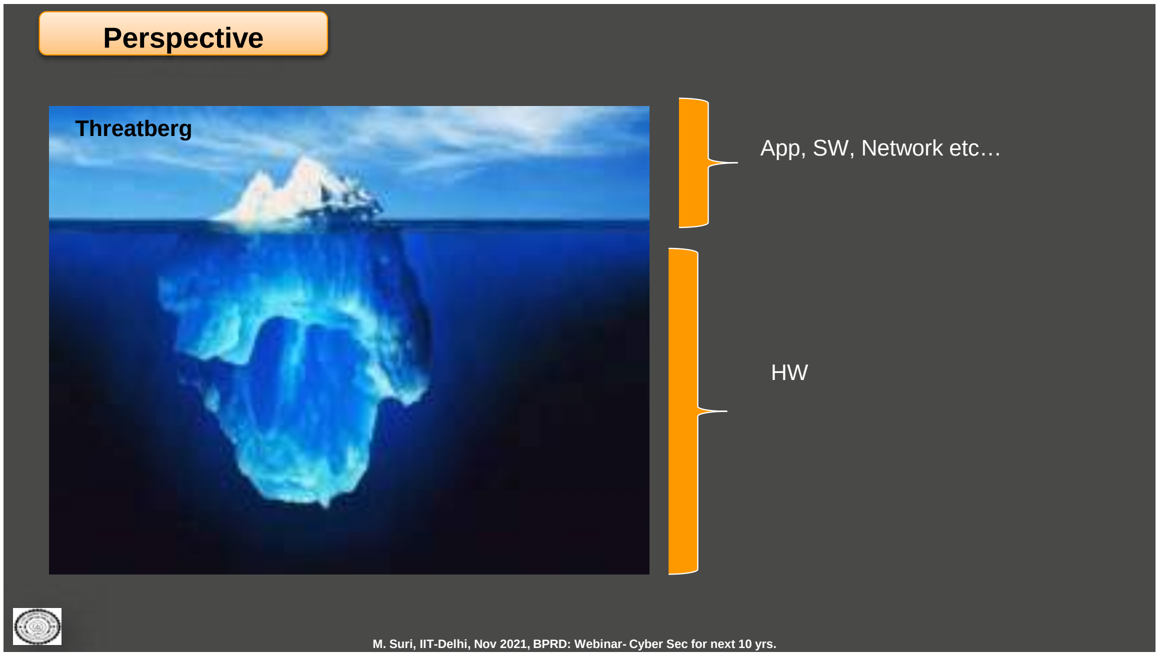
USD 475+ billion: 2018
USD 34.9 billion : March 2020

https://www.semiconductors.org/global-semiconductor-sales-decrease-3-6-percent-in-first-quarter-of-2020/

M. Suri, IIT-Delhi, Nov 2021, BPRD: Webinar- Cyber Sec for next 10 yrs.

Worldwide semiconductor revenue in 2018 was more than USD 475 billion and it went up to rise further making a month on month revenue close to USD 34.9 billion in March 2020.

While setting up the perspective of security threat posed by the vulnerabilities found in hardware, Dr Suri gave the example of threatberg. Threatberg is similar to iceberg in our common parlance. He explained that conventionally huge focus is given on software, application and network security which is actually just a tip of the iceberg and the real problem of cyber security lies with hardware.



Perspective

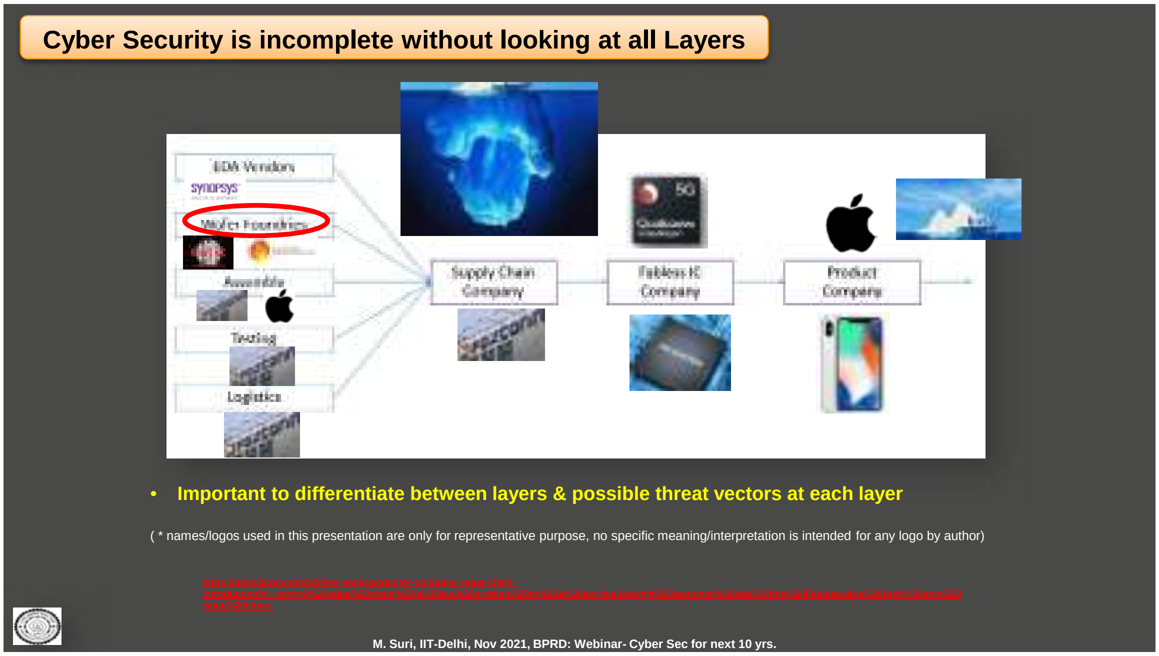
App, SW, Network etc…

HW

M. Suri, IIT-Delhi, Nov 2021, BPRD: Webinar- Cyber Sec for next 10 yrs.

He explained that hardware plays not just tactical threats for LEAs but also the strategic threats. Hardware originally plays a long term threat for the country as well as the LEAs.

Dr Suri further explained that how each layer involved in producing a final electronic product is important for everyone to understand so that possible threats at each layer can be properly realized for the LEAs to take necessary actions.



Cyber Security is incomplete without looking at all Layers

- Important to differentiate between layers & possible threat vectors at each layer

(* names/logos used in this presentation are only for representative purpose, no specific meaning/interpretation is intended for any logo by author)

https://anysilicon.com/fabless-semiconductor-company-value-chain-introduction/#:~:text=A%20value%20chain%20is%20a,a%20product%20or%20a%20service.&text=It%20assumes%20that%20the%20Fabless,also%20their%20own%20value%20chain.

M. Suri, IIT-Delhi, Nov 2021, BPRD: Webinar- Cyber Sec for next 10 yrs.

While looking at the above diagram, one can understand that a lot of focus is given on the security provided by the product company whereas the entire supply chain layer working behind the product company is largely overlooked. It is very important for LEAs to understand and differentiate between layers and possible threat vectors at each layer. Most of the time the vulnerabilities existing at the supply chain stage go undetected.

When we look at the hardware capacity worldwide, USA, Europe, Korea, Japan, Taiwan, Singapore and China are the leading hardware suppliers.

Moving forward, while discussing the security aspects of hardware, Dr Suri informed the audience that the US, Russia, China, EU, UK, Israel, Japan, Singapore, South Korea and Taiwan are world's strong nations with respect to core semi-hardware or semiconductor capability.

India's future cyber security matrix will be incomplete without hardware capacity.

While listing out the cyber security hardware threats, the professor listed out following threats/ vulnerabilities:

a. Backdoors

b. Trojans

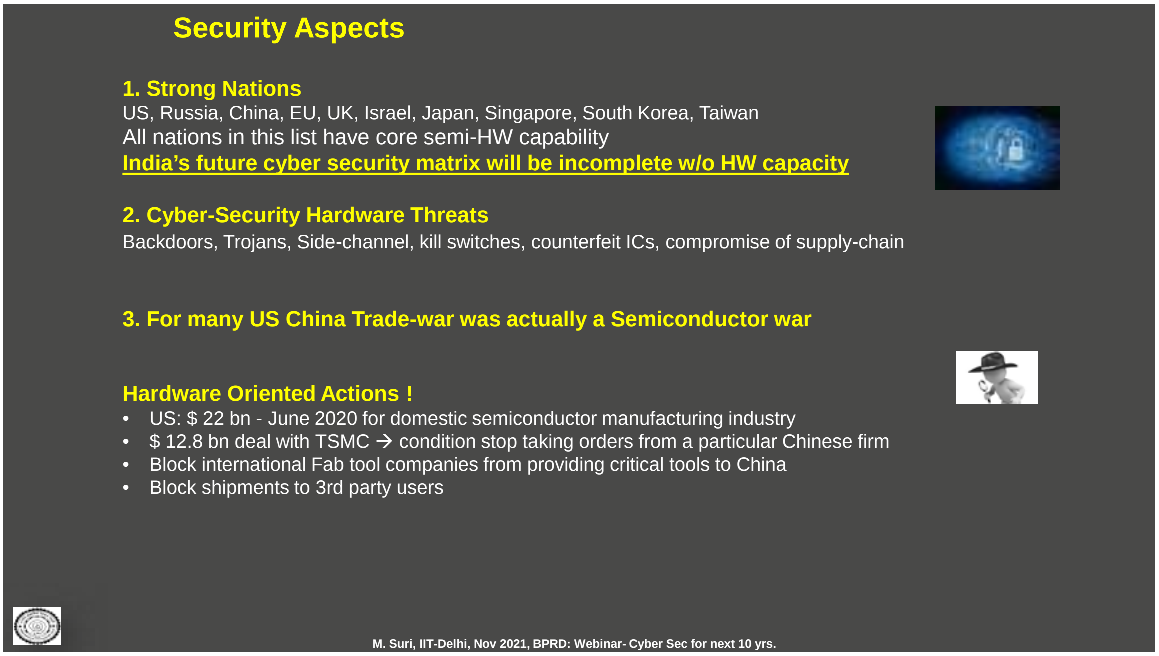
c. Side-channel

d. Kill Switches

e. Counterfeit Integrated Chips

f. Compromise of supply chain

Dr. Suri also touched upon the fact that semiconductor capabilities are the reason behind a lot of geopolitical activities happening across the globe and the trade war between US and China.



Security Aspects

1. Strong Nations
US, Russia, China, EU, UK, Israel, Japan, Singapore, South Korea, Taiwan
All nations in this list have core semi-HW capability
India's future cyber security matrix will be incomplete w/o HW capacity

2. Cyber-Security Hardware Threats
Backdoors, Trojans, Side-channel, kill switches, counterfeit ICs, compromise of supply-chain

3. For many US China Trade-war was actually a Semiconductor war

Hardware Oriented Actions !

- US: $ 22 bn - June 2020 for domestic semiconductor manufacturing industry
- $ 12.8 bn deal with TSMC → condition stop taking orders from a particular Chinese firm
- Block international Fab tool companies from providing critical tools to China
- Block shipments to 3rd party users

M. Suri, IIT-Delhi, Nov 2021, BPRD: Webinar- Cyber Sec for next 10 yrs.

Zero Trust is the modern cyber security model which talks about trusting no one in the cyber ecosystem. Dr. Suri explained the audience about zero security model as follows:

What is the most complex pillar of zero trust?

a. Trust no one & nothing

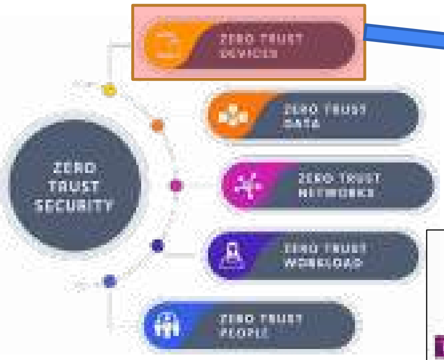
b. There is no trust zone

c. There is no safe zone

d. Identity is instantaneous

What is the most complex pillar of zero trust ?

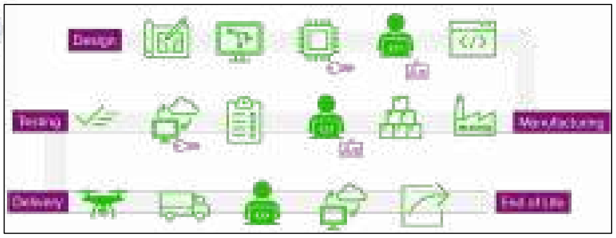
1. Trust no one & nothing !
2. There is no trust zone !
3. There is no safe zone !
4. Identity is instantaneous !



https://www.hkmci.com/zero-trust-security-model/

Devices – Hardware! – Physical Infra
Semiconductor - Electronics

- Capital
- Expertise
- Impact



Source: https://www.keyfactor.com/blog/webinar-recap-using-zero-trust-manufacturing-for-supply-chains/

M. Suri, IIT-Delhi, Nov 2021, BPRD: Webinar- Cyber Sec for next 10 yrs.

Zero Trust security model has several layers such as Zero Trust devices, Zero trust data, zero trust networks, zero trust workload and zero trust people.

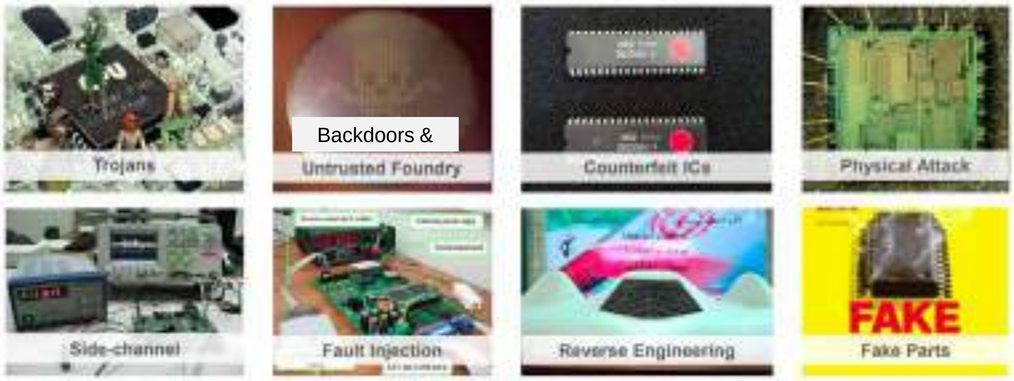
The Zero Trust Devices is a very crucial segment of zero trust security which is directly related to device hardware meaning semiconductors.

Developing semiconductor capabilities is a capital and expertise intensive area. Semiconductor industry has a very long Design, Testing and Delivery life cycle by the time it reaches the shape of a final product.

Dr. Suri emphasised on the estimates that in near future the hardware will have more and more threat domains.

Hardware Layer Threats to Zero Trust Model

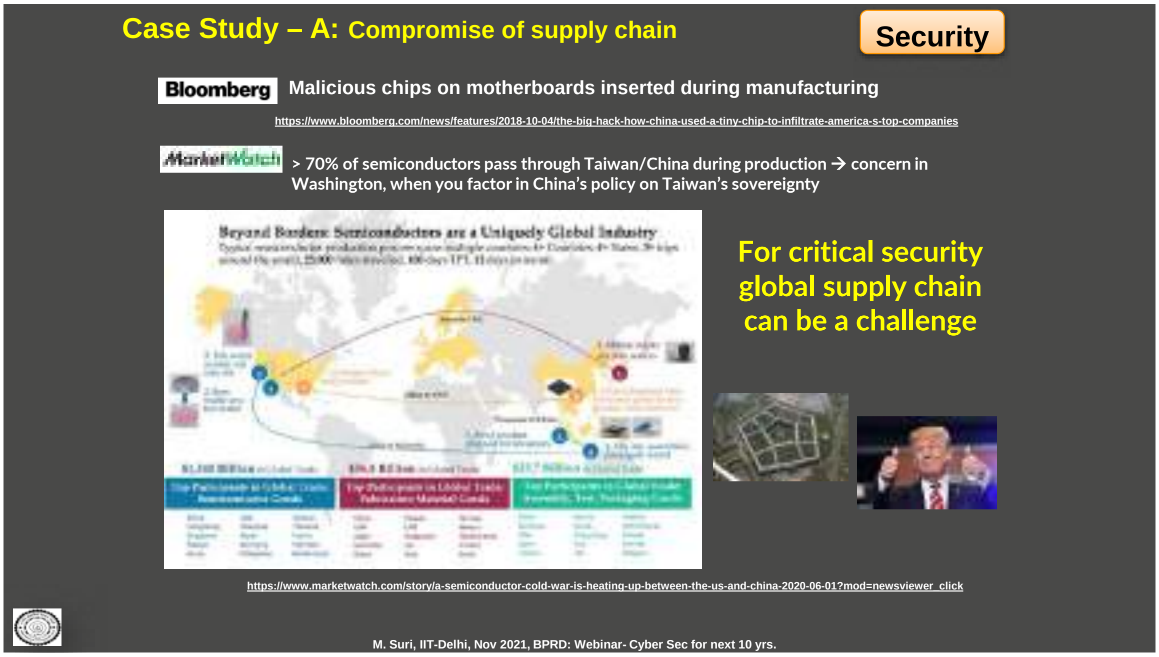
In the time to come domain of threat will be more & more in Hardware



Source: Mark M. Tehranipoor, Hardware Root-of-Trust for Cyber Security

M. Suri, IIT-Delhi, Nov 2021, BPRD: Webinar- Cyber Sec for next 10 yrs.

Dr. Suri also explained a few case studies to highlight the seriousness posed by the hardware aspect of cyber security.



Case Study – A: Compromise of supply chain

Security

Bloomberg Malicious chips on motherboards inserted during manufacturing

https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

MarketWatch > 70% of semiconductors pass through Taiwan/China during production → concern in Washington, when you factor in China's policy on Taiwan's sovereignty

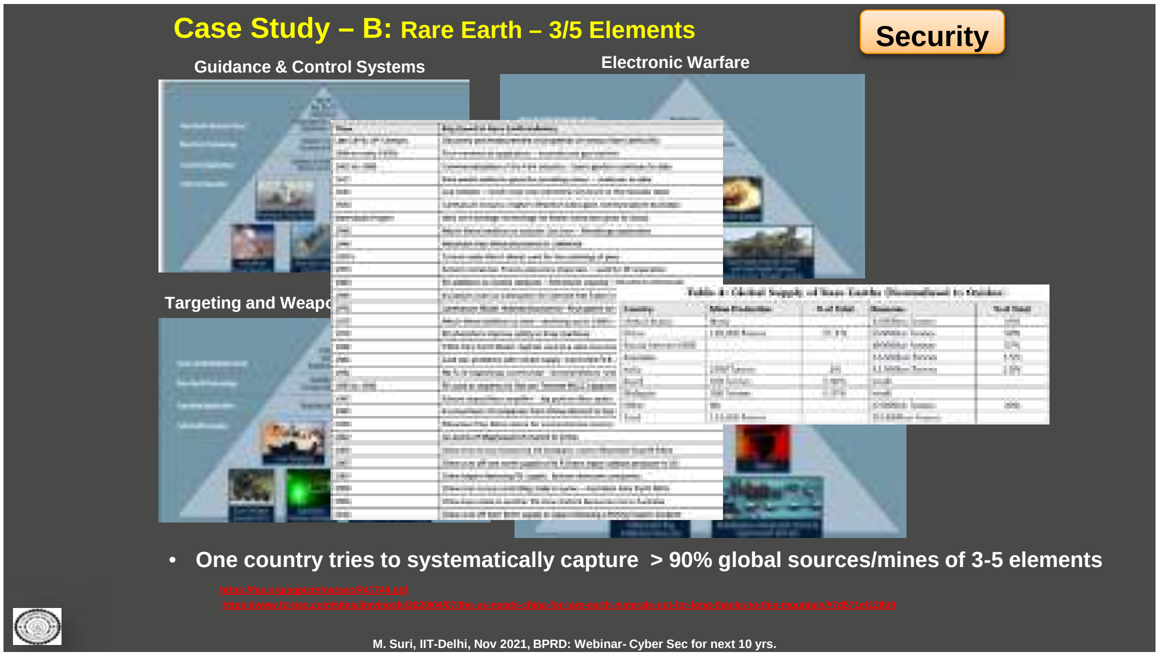
Beyond Borders: Semiconductors are a Uniquely Global Industry

For critical security global supply chain can be a challenge

https://www.marketwatch.com/story/a-semiconductor-cold-war-is-heating-up-between-the-us-and-china-2020-06-01?mod=newsviewer_click

M. Suri, IIT-Delhi, Nov 2021, BPRD: Webinar- Cyber Sec for next 10 yrs.

Few media reports suggest that malicious chips were inserted on motherboards during manufacturing. More than 70 percent of semiconductors pass through Taiwan and China. Therefore, the global supply chain can always be a challenge for critical infrastructure security.



Case Study – B: Rare Earth – 3/5 Elements

Security

Guidance & Control Systems

Electronic Warfare

Targeting and Weapo

Table 4: Global Supply of Rare Earths (Terminal) to Oxides

- One country tries to systematically capture > 90% global sources/mines of 3-5 elements

https://fas.org/sgp/crs/natsec/R41744.pdf

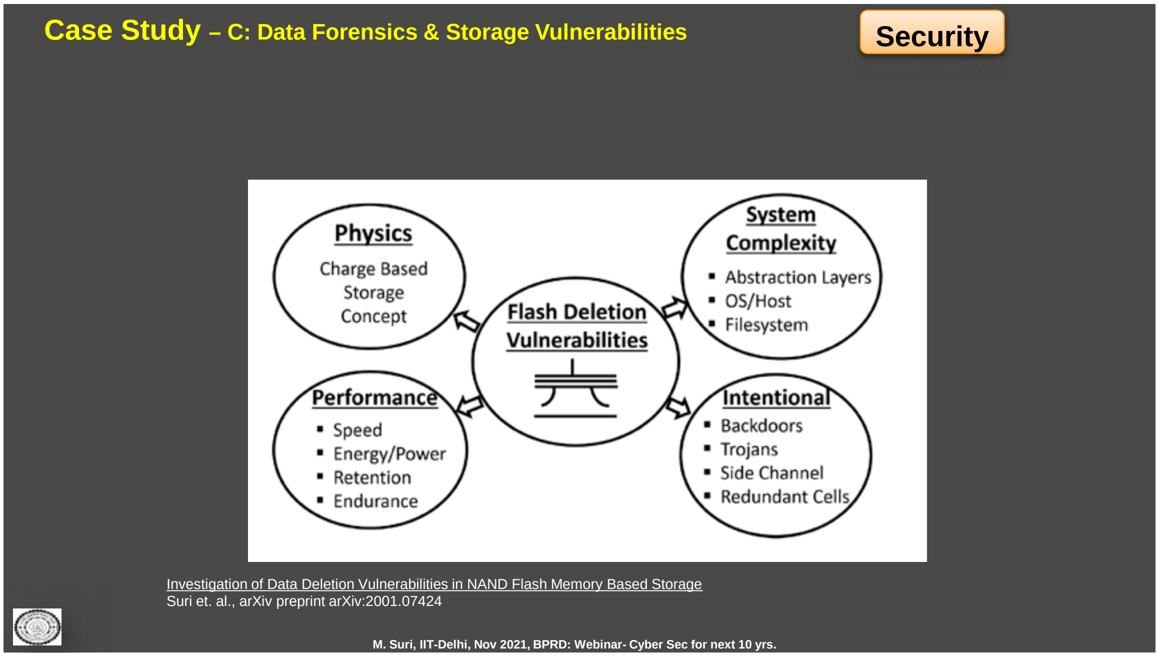
https://www.forbes.com/sites/jimvinoski/2020/04/07/the-us-needs-china-for-rare-earth-minerals-not-for-long-thanks-to-this-mountain/#7d571ef128b9

M. Suri, IIT-Delhi, Nov 2021, BPRD: Webinar- Cyber Sec for next 10 yrs.

The rare earth elements used for semiconductor manufacturing are also controlled by only a few countries.

The semiconductor is vital in nearly all strategic areas like Guidance and Control Systems, Electronic Warfare, Targeting and Weapon Systems and Communication.

The next case study discussed by Dr Suri is pertaining to Data Forensics and Storage Vulnerabilities.



Case Study – C: Data Forensics & Storage Vulnerabilities

Security

Physics
Charge Based Storage Concept

System Complexity
- Abstraction Layers
- OS/Host
- Filesystem

Flash Deletion Vulnerabilities

Performance
- Speed
- Energy/Power
- Retention
- Endurance

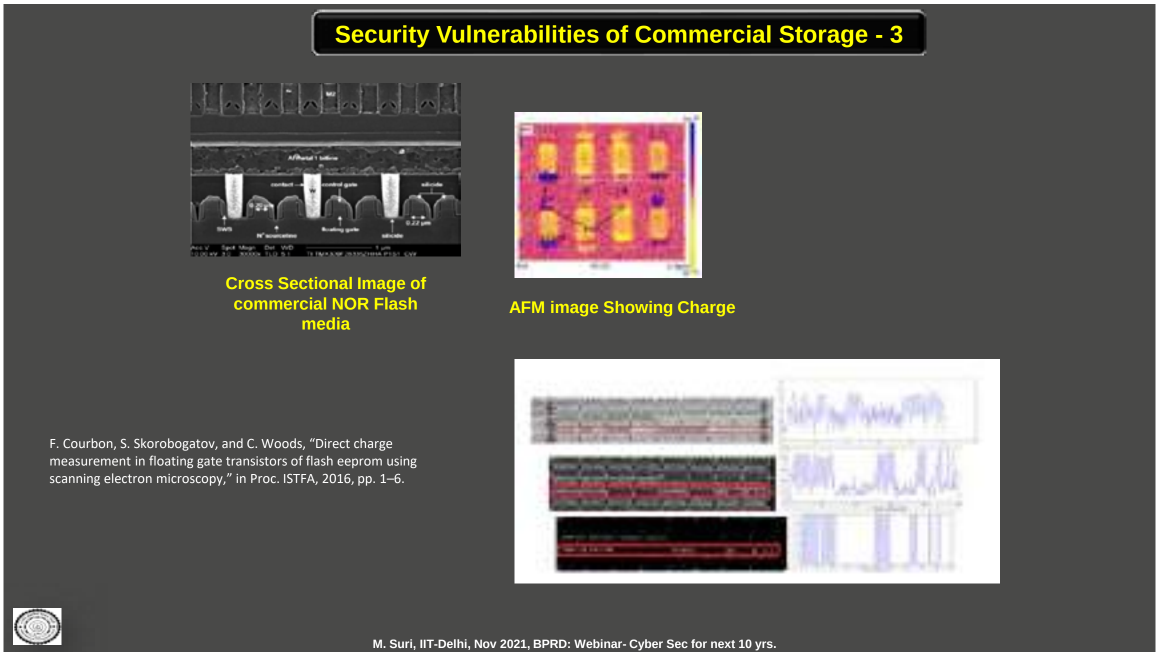
Intentional
- Backdoors
- Trojans
- Side Channel
- Redundant Cells

Investigation of Data Deletion Vulnerabilities in NAND Flash Memory Based Storage
Suri et. al., arXiv preprint arXiv:2001.07424

M. Suri, IIT-Delhi, Nov 2021, BPRD: Webinar- Cyber Sec for next 10 yrs.

System complexity, physics involved in manufacturing, performance related issues and intentional vulnerabilities are some of the flash drive deletion vulnerabilities. Digital forensics is largely related to data acquisition and data recovery which again falls back on flash drive deletion vulnerabilities.

In order to make sure that the right hardware is put in place, we need to build our capabilities in detection of hardware vulnerabilities. We need to understand that there are several ways to inject the vulnerabilities in hardware which go undetected by software scanning tools. Hardware vulnerabilities can be detected only through hardware.



Security Vulnerabilities of Commercial Storage - 3

Cross Sectional Image of commercial NOR Flash media

AFM image Showing Charge

F. Courbon, S. Skorobogatov, and C. Woods, "Direct charge measurement in floating gate transistors of flash eeprom using scanning electron microscopy," in Proc. ISTFA, 2016, pp. 1–6.

M. Suri, IIT-Delhi, Nov 2021, BPRD: Webinar- Cyber Sec for next 10 yrs.

Dr. Suri introduced some of the important work being done by IIT Delhi in the areas of hardware security. IIT Delhi is working on the Institute of Eminence Project on Secure Semiconductors and Nano hardware for critical Infrastructure. This project deals with following segments of research and development:

a. Semiconductor PUFs (physically unclonable functions)

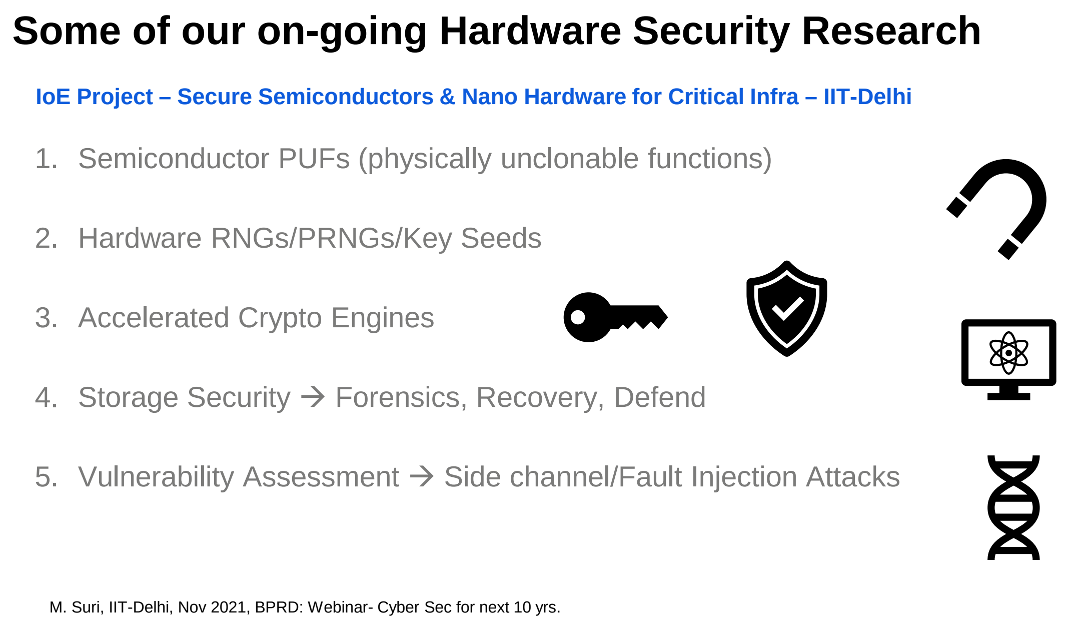
b. Hardware RNGs/PRNGs/Key Seeds

c. Accelerated Crypto Engines

d. Storage Security Forensics, Recovery, Defend

e. Vulnerability Assessment Side channel/Fault Injection Attacks

These projects will have extensive use cases for LEAs in coming years.

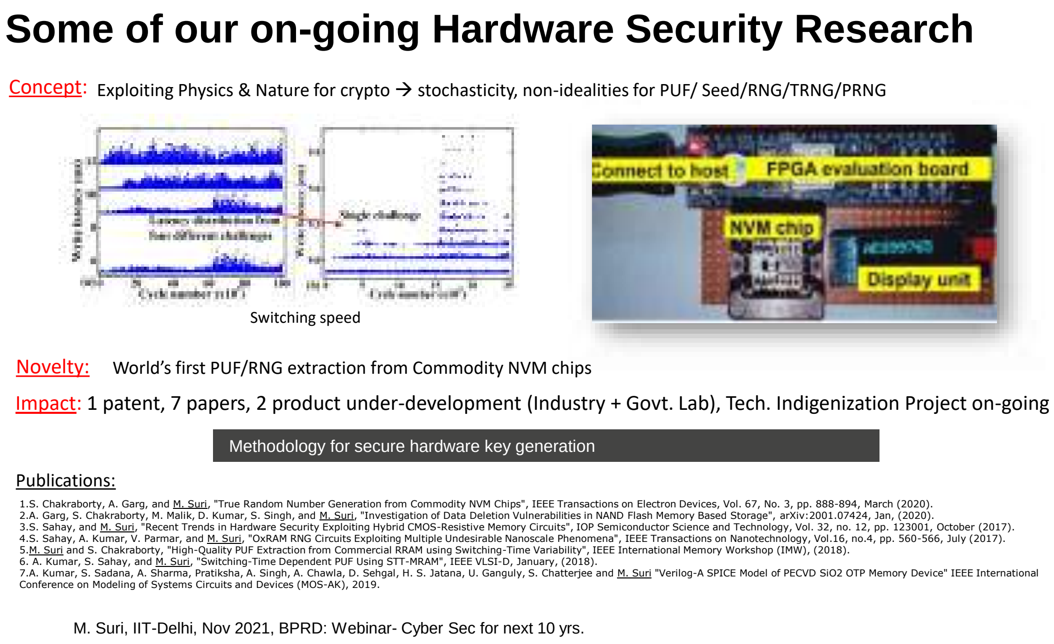


Some of our on-going Hardware Security Research

IoE Project – Secure Semiconductors & Nano Hardware for Critical Infra – IIT-Delhi

1. Semiconductor PUFs (physically unclonable functions)
2. Hardware RNGs/PRNGs/Key Seeds
3. Accelerated Crypto Engines
4. Storage Security → Forensics, Recovery, Defend
5. Vulnerability Assessment → Side channel/Fault Injection Attacks

M. Suri, IIT-Delhi, Nov 2021, BPRD: Webinar- Cyber Sec for next 10 yrs.



Some of our on-going Hardware Security Research

Concept: Exploiting Physics & Nature for crypto → stochasticity, non-idealities for PUF/ Seed/RNG/TRNG/PRNG

Latency distribution from two different challenges
Single challenge
Cycle number (x10⁴)
Switching speed
Connect to host
FPGA evaluation board
NVM chip
Display unit

Novelty: World's first PUF/RNG extraction from Commodity NVM chips

Impact: 1 patent, 7 papers, 2 product under-development (Industry + Govt. Lab), Tech. Indigenization Project on-going

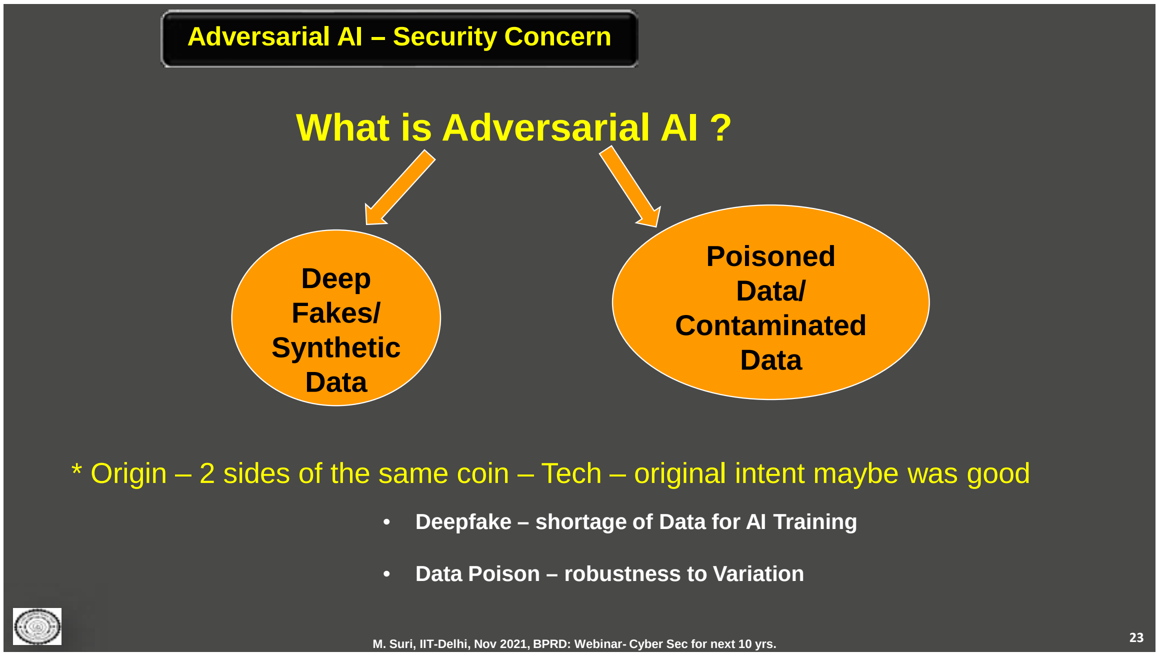
Methodology for secure hardware key generation

Publications:

1.S. Chakraborty, A. Garg, and M. Suri, "True Random Number Generation from Commodity NVM Chips", IEEE Transactions on Electron Devices, Vol. 67, No. 3, pp. 888-894, March (2020).
2.A. Garg, S. Chakraborty, M. Malik, D. Kumar, S. Singh, and M. Suri, "Investigation of Data Deletion Vulnerabilities in NAND Flash Memory Based Storage", arXiv:2001.07424, Jan, (2020).
3.S. Sahay, and M. Suri, "Recent Trends in Hardware Security Exploiting Hybrid CMOS-Resistive Memory Circuits", IOP Semiconductor Science and Technology, Vol. 32, no. 12, pp. 123001, October (2017).
4.S. Sahay, A. Kumar, V. Parmar, and M. Suri, "OxRAM RNG Circuits Exploiting Multiple Undesirable Nanoscale Phenomena", IEEE Transactions on Nanotechnology, Vol.16, no.4, pp. 560-566, July (2017).
5.M. Suri and S. Chakraborty, "High-Quality PUF Extraction from Commercial RRAM using Switching-Time Variability", IEEE International Memory Workshop (IMW), (2018).
6. A. Kumar, S. Sahay, and M. Suri, "Switching-Time Dependent PUF Using STT-MRAM", IEEE VLSI-D, January, (2018).
7.A. Kumar, S. Sadana, A. Sharma, Pratiksha, A. Singh, A. Chawla, D. Sehgal, H. S. Jatana, U. Ganguly, S. Chatterjee and M. Suri "Verilog-A SPICE Model of PECVD SiO2 OTP Memory Device" IEEE International Conference on Modeling of Systems Circuits and Devices (MOS-AK), 2019.

M. Suri, IIT-Delhi, Nov 2021, BPRD: Webinar- Cyber Sec for next 10 yrs.

Dr. Suri also explained about the adversarial challenges thrown away by Artificial Intelligence. Adversarial AI is a big security concern.



Adversarial AI – Security Concern

What is Adversarial AI ?

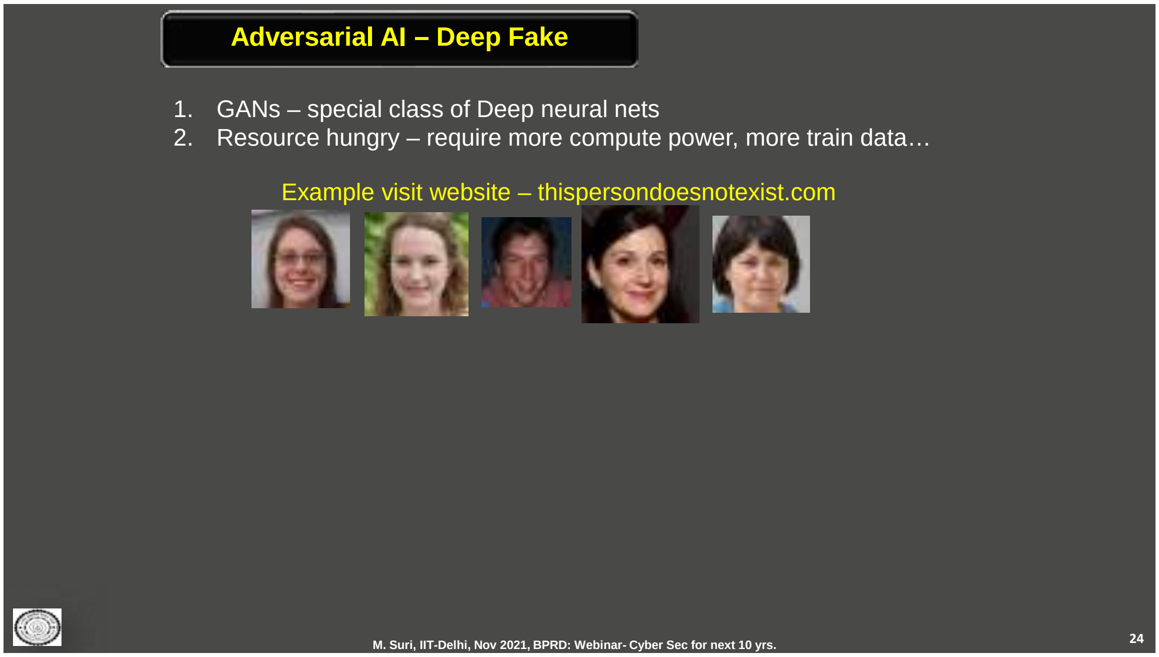
* Origin – 2 sides of the same coin – Tech – original intent maybe was good

- Deepfake – shortage of Data for AI Training
- Data Poison – robustness to Variation

M. Suri, IIT-Delhi, Nov 2021, BPRD: Webinar- Cyber Sec for next 10 yrs.

23

Deepfake audio, video and images are a cause of great concern for LEAs. It is a sophisticated form of AI technique through which two or more different videos/audios can be merged to give a malicious connotation to some incidents, personalities or news.



Adversarial AI – Deep Fake

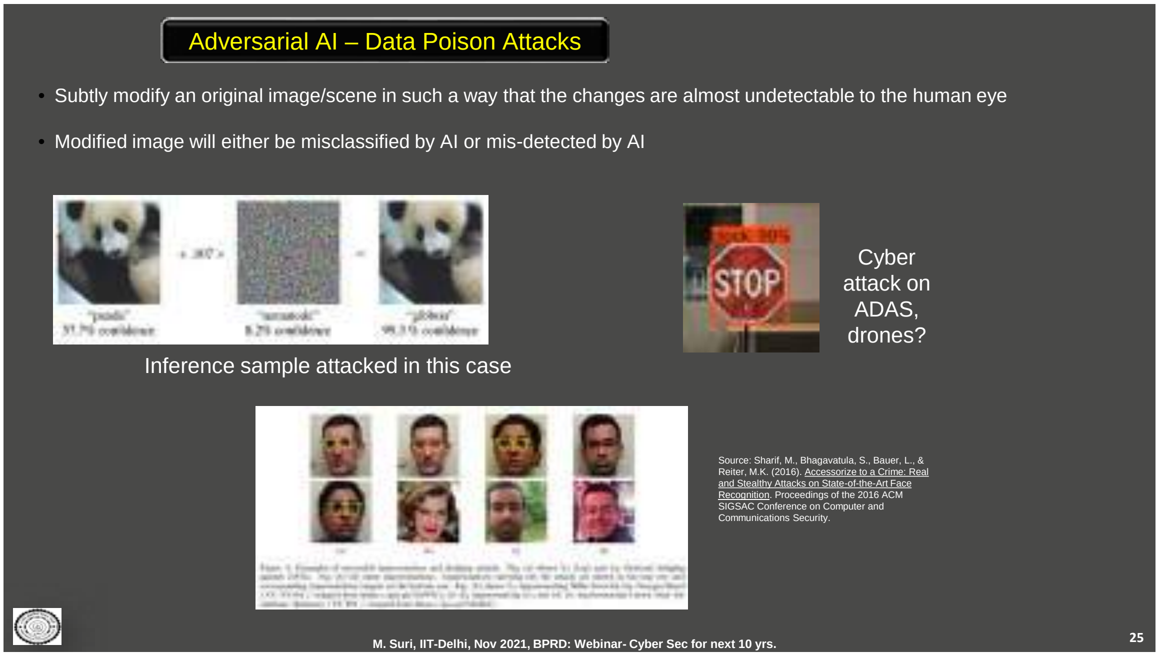
1. GANs – special class of Deep neural nets
2. Resource hungry – require more compute power, more train data…

Example visit website – thispersondoesnotexist.com

M. Suri, IIT-Delhi, Nov 2021, BPRD: Webinar- Cyber Sec for next 10 yrs.

24

In order to fight the menace of deepfake and other challenges posed by Adversarial AI, the LEAs need more and more hardware capabilities to train their detection models.



Adversarial AI – Data Poison Attacks

- Subtly modify an original image/scene in such a way that the changes are almost undetectable to the human eye
- Modified image will either be misclassified by AI or mis-detected by AI

+ .007 ×
=
"panda"
57.7% confidence
"nematode"
8.2% confidence
"gibbon"
99.3% confidence
STOP

Inference sample attacked in this case

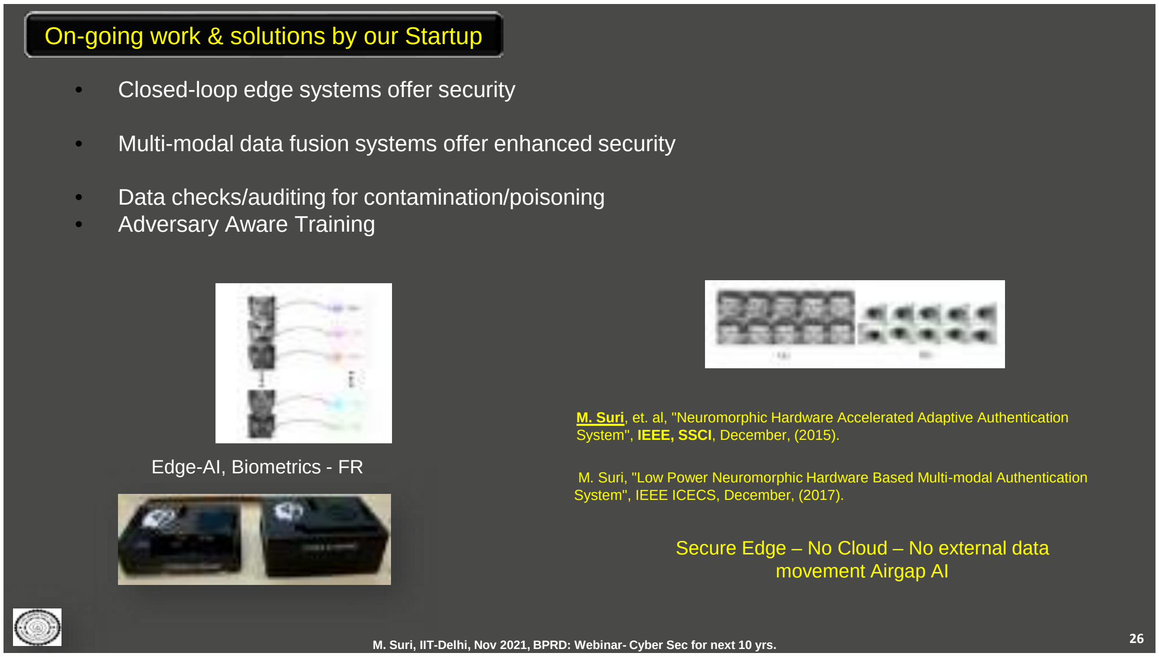
Cyber attack on ADAS, drones?

Source: Sharif, M., Bhagavatula, S., Bauer, L., & Reiter, M.K. (2016). Accessorize to a Crime: Real and Stealthy Attacks on State-of-the-Art Face Recognition. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security.

M. Suri, IIT-Delhi, Nov 2021, BPRD: Webinar- Cyber Sec for next 10 yrs.

25

Another form of Adversarial AI challenge is Data Poison Attacks through which original images can be changed in such a way that the changes go undetected by human eyes. Such things are rampantly used to generate fake news in social media and other internet platforms.



On-going work & solutions by our Startup

- Closed-loop edge systems offer security
- Multi-modal data fusion systems offer enhanced security
- Data checks/auditing for contamination/poisoning
- Adversary Aware Training

Edge-AI, Biometrics - FR

M. Suri, et. al, "Neuromorphic Hardware Accelerated Adaptive Authentication System", **IEEE, SSCI**, December, (2015).

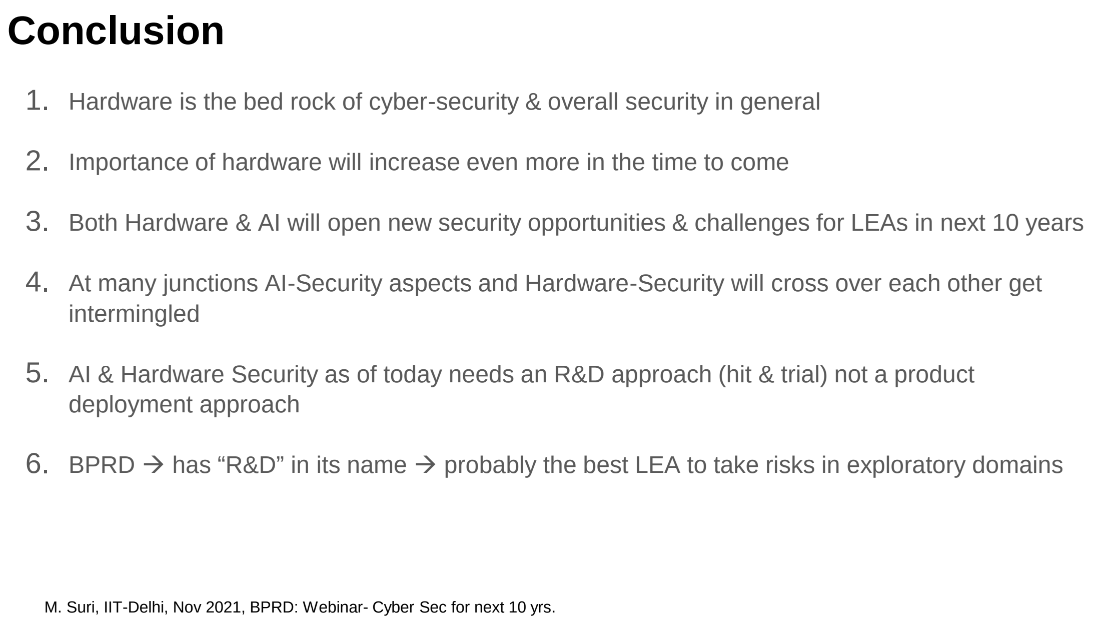
M. Suri, "Low Power Neuromorphic Hardware Based Multi-modal Authentication System", IEEE ICECS, December, (2017).

Secure Edge – No Cloud – No external data movement Airgap AI

M. Suri, IIT-Delhi, Nov 2021, BPRD: Webinar- Cyber Sec for next 10 yrs.

26

The startup founded by Dr. Manan Suri is working in the areas of closed-loop edge systems, multi modal data fusion systems to offer enhanced security, Data checks/auditing for contamination/poisoning and Adversary Aware Training.



Conclusion

1. Hardware is the bed rock of cyber-security & overall security in general
2. Importance of hardware will increase even more in the time to come
3. Both Hardware & AI will open new security opportunities & challenges for LEAs in next 10 years
4. At many junctions AI-Security aspects and Hardware-Security will cross over each other get intermingled
5. AI & Hardware Security as of today needs an R&D approach (hit & trial) not a product deployment approach
6. BPRD → has "R&D" in its name → probably the best LEA to take risks in exploratory domains

M. Suri, IIT-Delhi, Nov 2021, BPRD: Webinar- Cyber Sec for next 10 yrs.

Dr. Suri's talk ended with a brief session of open Q&A.

Session 3

Topic: Cyber Security Preparedness for next 10 years: LEA Perspective

Dr Balsing Rajput

Ph.D., DCP, Technology and Crime Prevention, Mumbai Police

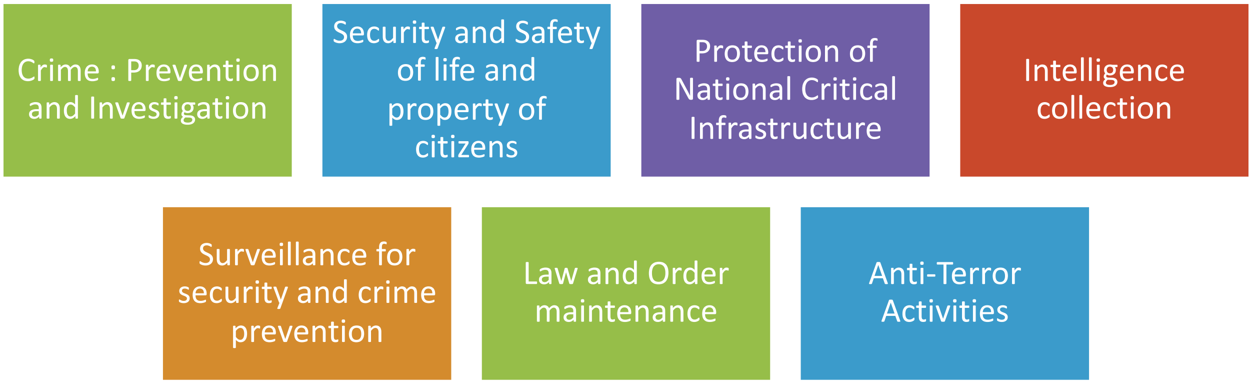
Dr. Balsing Rajput started his discussion on the given topic under following outline/aspect:

- Todays Cyberspace Scenario
- Law Enforcement Perspective
- Technologies shaping the next decade
- Emerging Cyber Threat Landscape
- Preparedness areas of LEA
- Preparedness : Way forward

He discussed about various points related to today's Technology Scenario in brief, including:

- Everything on cloud, whether it is in local or abroad domain
- IoT is everywhere
- AI and ML are running systems
- Convergence of platforms due to Mobile Technology
- OTT and Online service providers are there in every sector
- Encryption in Communication and data transfer
- Ultimately all these technologies are used by perpetrators to commit crime

He proposed various dimensions of Law Enforcement Preparedness Perspective like, Crime : Prevention and Investigation, Security and Safety of life and property of citizens, Protection of National Critical Infrastructure, Intelligence collection, Surveillance for security and crime prevention, Law and Order maintenance and Anti-Terror Activities.



Crime : Prevention and Investigation

Security and Safety of life and property of citizens

Protection of National Critical Infrastructure

Intelligence collection

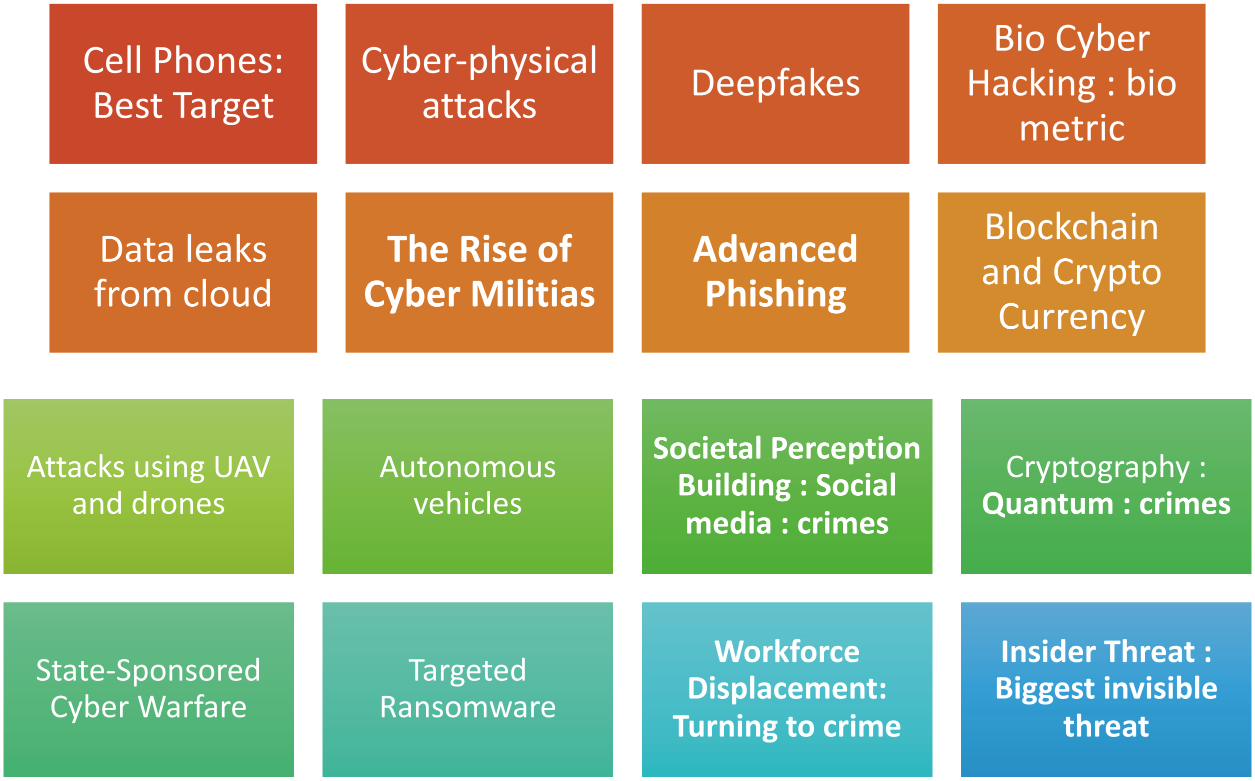
Surveillance for security and crime prevention

Law and Order maintenance

Anti-Terror Activities

He also discussed about various technologies that will shape the next decade, i.e. Artificial intelligence (AI) and machine learning, The Internet of Things (IoT), Wearables and Augmented devices, Big Data and real time analytics, Intelligent spaces, Homes, smart cities, Blockchains and cryptocurrencies, Cloud and edge computing Augmented reality and social media, Cell Phones: Ubiquitous, Autonomous vehicles, 5G Network, Drones and unmanned aerial vehicles, Quantum computing, Robotic process automation, 3D and 4D printing and additive manufacturing, Medical/Healthcare automation, Industry 4.0 etc.

Further, Dr. Rajput mentioned Emerging Cyber Threat Landscape as shown in the Figure below:



Cell Phones: Best Target

Cyber-physical attacks

Deepfakes

Bio Cyber Hacking : bio metric

Data leaks from cloud

The Rise of Cyber Militias

Advanced Phishing

Blockchain and Crypto Currency

Attacks using UAV and drones

Autonomous vehicles

Societal Perception Building : Social media : crimes

Cryptography : **Quantum : crimes**

State-Sponsored Cyber Warfare

Targeted Ransomware

Workforce Displacement: Turning to crime

Insider Threat : Biggest invisible threat

Dr. Rajput suggested following Preparedness Areas in order to deal with Emerging Cyber Threat Landscape:

- Institutional/organization developments
- Legal and compliance frameworks
- Technology development
- Processes and techniques
- Cooperation and information sharing
- Research and innovation
- Human resource development
- Capacity building and adaptation
- Operational Technology
- Anti Terror Measures
- Cyber Espionage and intelligence

Institutional / organization developments

Legal and compliance frameworks

Technology development

Processes and techniques

Cooperation and information sharing

Research and innovation

Human resource development

Capacity building and adaptation

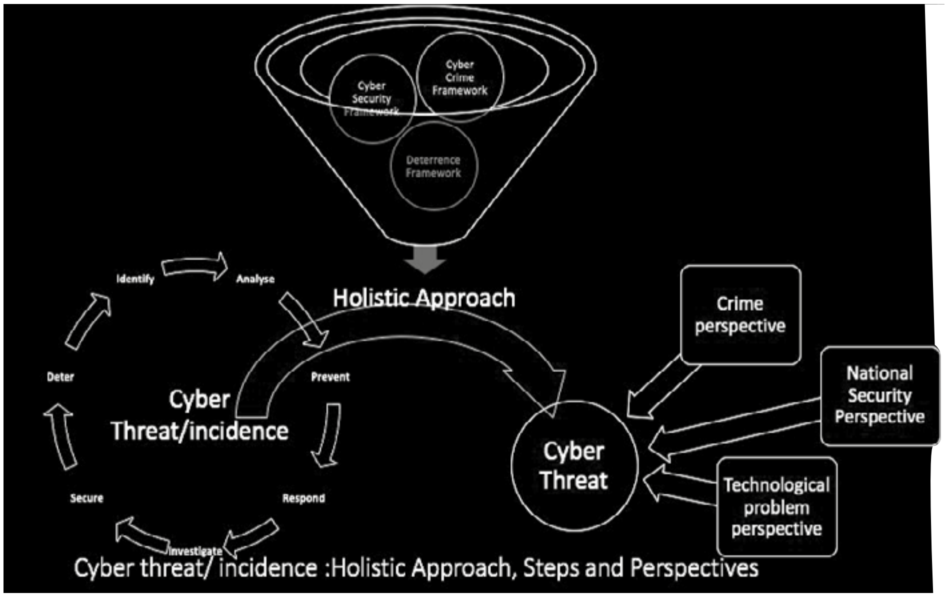
Operational Technology

Anti Terror Measures

Cyber Espionage and intelligence

The Model for Preparedness Adoption should be Integrated, Automated, Collaborative mechanism, Integrated, Mature and Resilient.

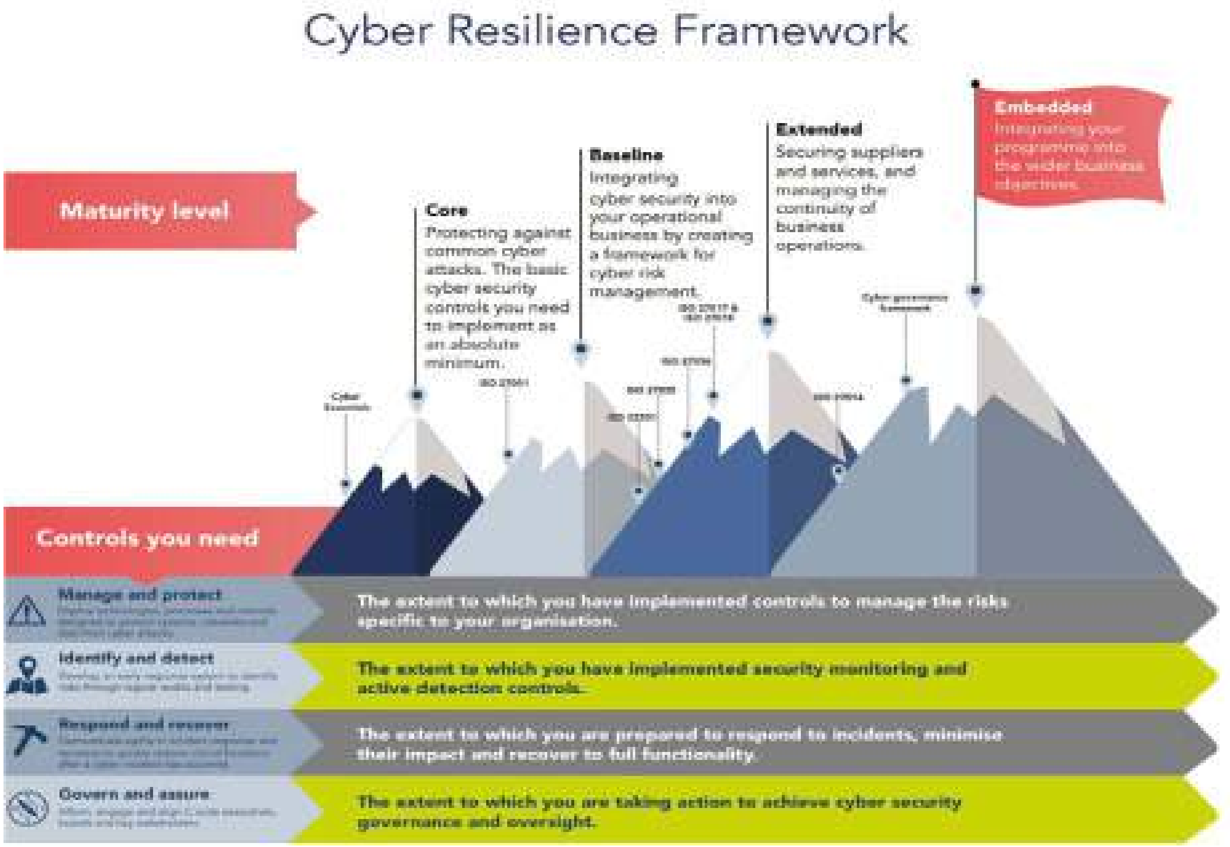
He discussed about the Holistic and Integrated Approach as shown in the Figure below:



Cyber threat/ incidence :Holistic Approach, Steps and Perspectives

The following AIM -Achieving Resilience Framework is discussed during the talk.

Framework Model



Core
Protecting against common cyber attacks. The basic cyber security controls you need to implement as an absolute minimum.

Baseline
Integrating cyber security into your operational business by creating a framework for cyber risk management.

Extended
Securing suppliers and services, and managing the continuity of business operations.

Embedded
Integrating your programme into the wider business objectives.

The extent to which you have implemented controls to manage the risks specific to your organisation.

The extent to which you have implemented security monitoring and active detection controls.

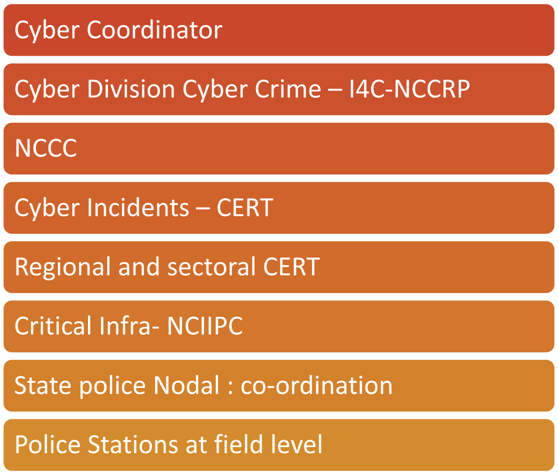
The extent to which you are prepared to respond to incidents, minimise their impact and recover to full functionality.

The extent to which you are taking action to achieve cyber security governance and oversight.

Strategies and Policies which needs in place are:

- Asset management
- Vulnerability Management
- Threat management
- Incident management
- Continuity management
- Crisis management
- Disaster management

Preparedness for the Organizational and Operational Structure Developed is based on following points:



Cyber Coordinator

Cyber Division Cyber Crime – I4C-NCCRP

NCCC

Cyber Incidents – CERT

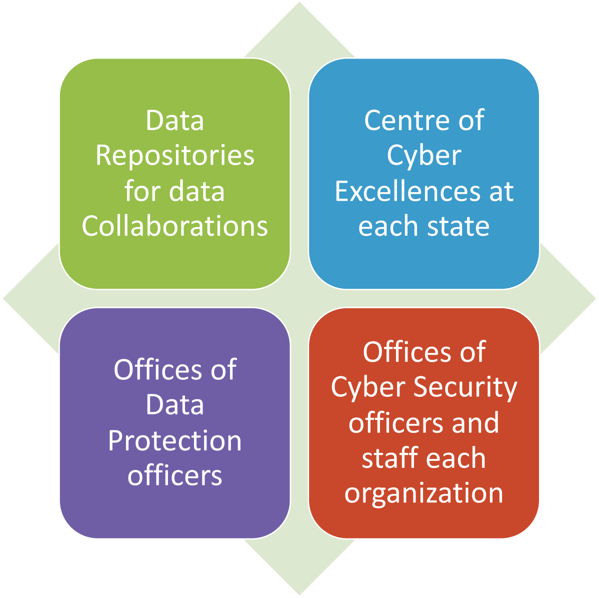
Regional and sectoral CERT

Critical Infra- NCIIPC

State police Nodal : co-ordination

Police Stations at field level

The new Organizational Framework need to build as follows:



Data Repositories for data Collaborations

Centre of Cyber Excellences at each state

Offices of Data Protection officers

Offices of Cyber Security officers and staff each organization

Preparedness for Technology development includes following points:

- Digitization of Police operations
- Enterprise Resource Solutions for Police (ERP)
- Mobile Policing for Faster Response
- Fusion Centers : predictive policing
- Analysis Laboratories in each district
- Anti Drone Solutions

Preparedness for Legal and Compliance frameworks includes following points:

- Data Protection Laws
- Cyber Security Law
- Amendments in IT Act
- Autonomous Vehicles and UAV
- AI and Robots : legal Framework
- Cryptocurrency legal framework

Preparedness for Processes and Techniques includes:

- SOP for Cyber Crime and future Crimes
- Forensic and investigation processes for new tech
- Standardization and setting Norms

Preparedness for Cooperation and information sharing includes:

1. Collaboration Portal:

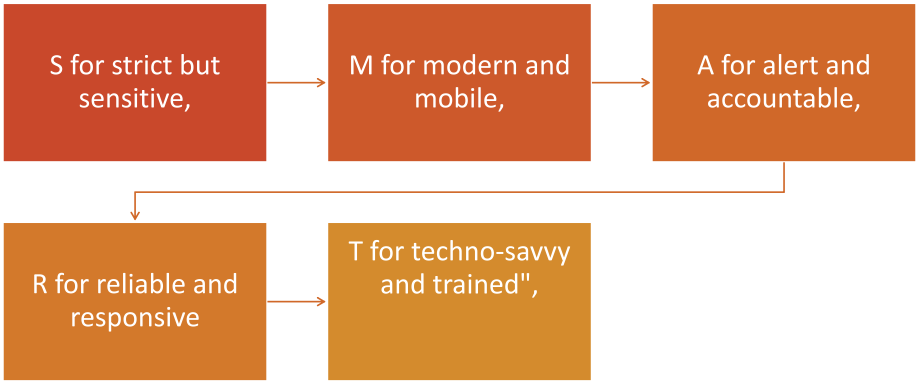
    - Integrated portal for data sharing within LEA and state

- Help and coordinated ops
- Accused info and support during ops

2. Platform for information Fetching from Intermediaries:

- Integrated portal for all LEA to call from intermediaries
- All notices and data requests to flow through this
- Can follow data queries and responses of Intermediaries and service providers

Finally, Dr. Rajput mentioned the ‘SMART’ Policing will be the way forward for the Cyber Security Preparedness for next decade. The word ‘SMART’ includes:



S for strict but sensitive,

M for modern and mobile,

A for alert and accountable,

R for reliable and responsive

T for techno-savvy and trained",

Dr. Balsing Rajput’s talk ended with a brief session of open Q&A.

Contact List of BPR&D Officers

Name of the Officer	Ph. No.
Sh. Karuna Sagar IG / Director (Mod)	011- 26782023
Sh. Navrattan Joshi PSO (Electronics)	011-26782185
Lt. Col. Ashwani Kumar AD (Mod)	011- 26782183
Dr. Ajit Mukherjee PSO (LS)	011- 26734938
Dr. Raveesh Kumar PSO (W)	011- 26785451
Sh. Sushil Kumar PSO (B&E)	011-26734931
Dr. M.M. Gosal SSO (T)	011- 26734815

References

1. Investigation of Data Deletion Vulnerabilities in NAND Flash Memory Based Storage Suri et. al., arXiv preprint arXiv:2001.07424

2. F. Courbon, S. Skorobogatov, and C. Woods, "Direct charge measurement in floating gate transistors of flash eeprom using scanning electron microscopy," in Proc. ISTFA, 2016, pp. 1–6.

3. S. Chakraborty, A. Garg, and M. Suri, "True Random Number Generation from Commodity NVM Chips", IEEE Transactions on Electron Devices, Vol. 67, No. 3, pp. 888-894, March (2020).

4. A. Garg, S. Chakraborty, M. Malik, D. Kumar, S. Singh, and M. Suri, "Investigation of Data Deletion Vulnerabilities in NAND Flash Memory Based Storage", arXiv:2001.07424, Jan, (2020).

5. S. Sahay, and M. Suri, "Recent Trends in Hardware Security Exploiting Hybrid CMOS-Resistive Memory Circuits", IOP Semiconductor Science and Technology, Vol. 32, no. 12, pp. 123001, October (2017).

6. S. Sahay, A. Kumar, V. Parmar, and M. Suri, "OxRAM RNG Circuits Exploiting Multiple Undesirable Nanoscale Phenomena", IEEE Transactions on Nanotechnology, Vol.16, no.4, pp. 560-566, July (2017).

7. M. Suri and S. Chakraborty, "High-Quality PUF Extraction from Commercial RRAM using Switching-Time Variability", IEEE International Memory Workshop (IMW), (2018).

8. A. Kumar, S. Sahay, and M. Suri, "Switching-Time Dependent PUF Using STT-MRAM", IEEE VLSI-D, January, (2018).

9. A. Kumar, S. Sadana, A. Sharma, Pratiksha, A. Singh, A. Chawla, D. Sehgal, H. S. Jatana, U. Ganguly, S. Chatterjee and M. Suri "Verilog-A SPICE Model of PECVD SiO2 OTP Memory Device" IEEE International Conference on Modeling of Systems Circuits and Devices (MOS-AK), 2019.

10. https://www.iacis.com/training/basic-computer-forensics-examiner/

11. http://www.digitalrecordsforensics.org/drf_links.cfm?cat=org

12. https://www.swgde.org/home

13. Digital Forensics and Investigations by Jason Sachowski, CRC Press

14. https://onlinelibrary.wiley.com/doi/epdf/10.1002/spy2.123

15. https://www.semiconductors.org/global-semiconductor-sales-decrease-3-6-percent-in-first-quarter-of-2020/

16. https://www.keyfactor.com/blog/webinar-recap-using-zero-trust-manufacturing-for-supply-chains/

17. Mark M. Tehranipoor, Hardware Root-of-Trust for Cyber Security

18. https://www.marketwatch.com/story/a-semiconductor-cold-war-is-heating-up-between-the-us-and-china-2020-06-01?mod=newsviewer_click

19. https://fas.org/sgp/crs/natsec/R41744.pdf

20. https://www.forbes.com/sites/jimvinoski/2020/04/07/the-us-needs-china-for-rare-earth-minerals-not-for-long-thanks-to-this-mountain/#7d571ef128b9

21. Sharif, M., Bhagavatula, S., Bauer, L., & Reiter, M.K. (2016). Accessorize to a Crime: Real and Stealthy Attacks on State-of-the-Art Face Recognition. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security.

22. M. Suri, et. al, "Neuromorphic Hardware Accelerated Adaptive Authentication System", IEEE, SSCI, December, (2015).

23. M. Suri, "Low Power Neuromorphic Hardware Based Multi-modal Authentication System", IEEE ICECS, December, (2017).

officialBPRDIndia

BPRDIndia

Bureau of Police Research & Development India

bprdIndia

www.bprd.nic.in

Cyberdost

www.cybercrime.gov.in

Indian Cyber Crime Coordination Centre

NATIONAL CYBER CRIME RESEARCH & INNOVATION CENTRE (NCR&IC)
BUREAU OF POLICE RESEARCH AND DEVELOPMENT
Ministry of Home Affairs, Government of India
NH-8, Mahipalpur, New Delhi-110037

RAMA KRISHNA TRADERS, Delhi