National Cyber Security Scholar Program

JOINT CERTIFICATION

MDI, Gurugram
Management Development Institute (MDI) Gurugram, has been a trendsetter in the field of management education, consulting, high quality research and executive development. The institute has the distinction of being the first internationally accredited Indian Business School having received international accreditation by Association of MBAs (AMBA) London in 2006.

ISAC, New Delhi
The ISAC foundation is a PPP with National Critical Information Infrastructure Protection Center (**NCIIPC**), Government of India, a nodal agency under IT Act, Section 70A, for the protection of CII and cybersecurity capacity building.

Brief: The cybersecurity scholar program is a comprehensive and insightful course for the next generation cybersecurity leaders & Policymakers and jointly conducted by Management Development Institute (MDI), Gurugram, and Information Sharing and Analysis Center (ISAC).

Participants: Senior central/state/PSU *officers, CEOs, CXOs, CFOs, CISOs, CIOs and Senior Faculty*

Duration: 8 Week online program

2020 Schedule: Primary Lectures will be held on the following dates from 3 PM to 5 PM:

- **16th August**
- **23rd August**
- **30th August**
- **6th September**
- **13th September**
- **20th September**
- **27th September**
- **4th October**

Secondary / Guest lectures will be scheduled as live webinars and made available on the e-learning platform.

The need for the program:

Why do certain companies win against hackers, and why do others fail? What will state-sponsored attacks in the global economy mean for your organization? How can you defend against next-generation cyberattacks by continually being one step ahead?

Eight weeks at the ISAC Executive Program, in collaboration with MDI, will immerse you in new ways of thinking and insights that will propel your career and greatly enhance your company defenses against emerging cyber-attacks. Learn to strengthen enterprise cybersecurity, explore emerging trends, and transform them into actionable insights.

According to a Nasscom, Data Security Council of India & PwC Report, the cybersecurity market has been projected to be $35 billion by 2025. The biggest customers will be various Government departments, LEAs, and Intelligence agencies across the world.

This scholar program aims to bridge the gap at the leadership level to drive the initiatives and business opportunities in both the Government and the Industry.

Program Objectives

Enhancing National Security

The National Cyber Security Scholar program aims to create next-generation thought leaders in cybersecurity. Lead the initiatives at the national level for skill-building in emerging technologies, drive large scale programs that protect organizations from cyber threats, implement and drive projects of national importance on cybersecurity, and help create resilience in cyberspace of the country.

The professionals who complete this program will be deemed national assets under the National Security Program and provided a Level 4 security clearance of ISAC.

Learn to build, manage, and deliver enterprise security even under the most pressing challenges in this eight-week executive program.

This scholar program looks at this intricate relation between technology, national security, cyber warfare, and its impact on your organization and business.

Cyber Warfare is a highly asymmetrical form of War strategy rendering the enemy paralyzed within a matter of a few minutes. We will look at the most pressing security challenges faced by the Indian administration, intelligence agencies, the private sector, and even every individual to an extent.

The course will also cover a wide variety of topics ranging from terrorist ideologies, cyber threats, threats to critical infrastructure, intelligence challenges, underground web, diplomacy and foreign policy, legal aspects of terrorism, tools for hacking, and future of national security and cyber warfare.

Who Should Attend

- Senior-level leaders at Government departments / bodies responsible for homeland and cybersecurity operations.
- Senior-level leaders at large companies who are responsible for cybersecurity
- Senior faculty and professors who are responsible for driving emerging technologies including next-generation courses in Cybersecurity, AI&ML, IoT and Cloud computing to build capacity and meet Industry needs
- Seasoned and influential executives at Managed Security Services Providers (MSSPs) who will use this opportunity to make an even more significant difference in their careers and their organizations' futures.
- Minimum Five years of relevant Industry / Government experience.
- **Suitable for eligible and experienced professionals who are looking for a second career option.**

Delivered using world-class technology

VIRTUAL LABS AND REAL-WORLD SIMULATION

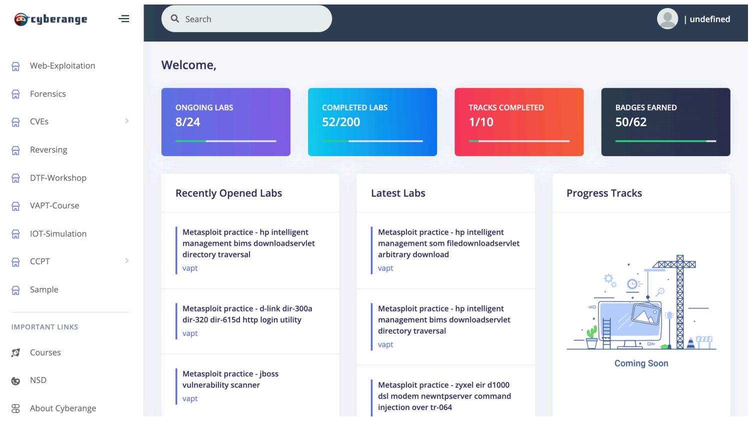
Credibility:

Tech Incubated by ISAC foundation and is the world's first Cyber Physical System (CPS) based on Industry 4.0.

Established in NCIIPC, Prime Minister's Office, for conducting Hackathon for the Prestigious GCCS 2017 Conference with over 120 countries participating in the Hackathon.

Used by large organizations in Cyber Security for creating next generation workforce on IoT, SCADA Security, Cyber Security, Artificial Intelligence and Machine Learning.

The program is delivered using world-class technology that combines virtual and physical-based simulation to practice the latest attack vectors. You will access individual virtual machines designed with vulnerabilities and technical challenges reflecting real-world deployments.



Welcome,

ONGOING LABS 8/24

COMPLETED LABS 52/200

TRACKS COMPLETED 1/10

BADGES EARNED 50/62

Recently Opened Labs

Metasploit practice - hp intelligent management bims downloadservlet directory traversal
vapt

Metasploit practice - d-link dir-300a dir-320 dir-615d http login utility
vapt

Metasploit practice - jboss vulnerability scanner
vapt

Latest Labs

Metasploit practice - hp intelligent management som filedownloadservlet arbitrary download
vapt

Metasploit practice - hp intelligent management bims downloadservlet directory traversal
vapt

Metasploit practice - zyxel eir d1000 dsl modem newntpserver command injection over tr-064

Progress Tracks

Top 10 benefits of the technology

1. Fully available on the cloud
2. Predefined setup of labs, saving your time
3. No clean up and reset required after practicing labs
4. No risk of malwares affecting corporate network
5. Instant access to labs for training
6. Updated every month with latest CVEs
7. Get hands-on training on real-world scenarios
8. World class labs with enterprise applications
9. Consoles pre-installed with all required software, tools and code for cyber security training and hands-on practice
10. Get full access to labs at the comfort of your homes after training hours.

Learning Outcomes

PROGRAM STRUCTURE

Participants admitted to the 8-week program already hold significant positions and responsibilities.

To accommodate their time constraints, the program requires delegates to attend lectures only once a week for eight weeks for the whole program.

Delegates complete their research and coursework via the web and **require approximately 7 to 8 hours per week.**

The program uses a "blended" learning approach in the delivery of course material and learning experiences.

During the week, participants will receive reading material to analyze and evaluate. Additionally, participate in threaded discussions on the weeks' topics. During regular sessions every week, the participants will spend their time engaged in intensive lectures, case studies, debates, and readings.

Upon completion of the course you will be able to:

1. Comprehend the macro level cyber security issues and the convergence with National Security.
2. Evaluate the importance of cyber security; understand the cyber risks to national and international security in developing and developed states.
3. Identify the risks of cybercrime, cyber terrorism, and cyber war.
4. Evaluate different paradigms for cyber security and determine the approach that best applies in an individual country.
5. Assess the strengths and weaknesses of the various international and national cyber security strategies.
6. Understand the role of government and the private sector in cyber security and critical infrastructure protection.
7. Develop strategies, plans and programs to prevent terrorist attacks within India, and reduce India's vulnerability to terrorism;
8. Help various agencies in India improve homeland security preparedness by conducting "real world" actionable policy and strategy development.

Course Outline

BLENDED APPROACH

Online collaborative tools such as forums, wikis, blogs, and messaging facilitate discussion, debate and collaboration among program participants and faculty. Course materials are easily accessible online in various forms, including streaming media lectures, audio recordings of required readings, printed text, and more.

Delegates engage in active learning through exercises, use case studies, and simulations; Delegates apply their newly gained theoretical insights and analytic skills in a risk-free environment where strategies and policies can be tested.

Delegates complete research papers and a thesis on actual issues confronting their state, city or sponsoring organizations.

The following topics will be covered:

Week	Module	Title
Week 1	NCS 101	Critical Information Infrastructure (CII) and National Security
Week 2	NCS 102	Smart Cites and Homeland Security of India
Week 3	NCS 103	Economy and National Security
Week 4	NCS 104	Electronic Contamination and Cyber Warfare
Week 5	NCS 105	Intelligence and National Security
Week 6	NCS 106	Digital Forensics, Legal System and Privacy Challenges in India
Week 7	NCS 107	Artificial Intelligence and Machine Learning
Week 8	NCS 108	Interaction with Law enforcement and Intelligence Agencies

NSD Scholars research on policy-relevant topics and international cyber security issues. They join other distinguished scientists, social scientists, engineers and cyber security researchers who work together on security problems that need interdisciplinary and collaborative approach. NSD scholars address overlapping issues in cyber security, economic security; homeland security; intelligence; capacity building and effective global engagement.

Detailed course outline in Annexure A

Program Fees

The course is available in the following plans:

Plan	**Fee**	**Description**
MDI Campus	INR 2,50,000	Course delivered on MDI Gurugram campus with 5 days of stay on campus. **(Not offered currently due to Covid-19)**
Online	**INR 1,20,000**	**Program fully delivered online.**
Online – For Academic Institutions	INR 60,000	Concession for existing faculty/professors working at AICTE or UGC approved Institutions

Excludes all applicable taxes.

Please refer to Annexure B for Payment details.

About Information Sharing and Analysis Center (ISAC)

ISAC is India's leading non-profit foundation committed to securing the cyber space of the nation by providing credible platforms for Information Sharing & capacity development. ISAC is a partner with **Indian Computer Emergency Response team** (CERT-IN) under Ministry of Electronics and Information Technology and the **All India Council for Technical Education** (AICTE), under Ministry of Human Resources and Development.

ISAC manages the **National Security Database** (NSD), a prestigious certification program awarded to credible & trustworthy Information security experts with proven skills to protect the National Critical Infrastructure & economy of the country. The program is supported by the Prime Minister's Office, Government of India.

The ISAC foundation has an MoU with All India Council of Technical Education (AICTE) for:

- Creation 100,000 cyber security professionals under the National Security Database program
- Establishment of Centers of Excellence in Cyber Security based on Cyberange ® Smart City Simulator across India
- Training on ethics for AICTE approved institutions to enhance workplace ethics
- Faculty Development Program

Annexure A

DETAILED COURSE OUTLINE

Table of Contents

Week 1 – CII and National Security

In this Module, we will look at Critical Infrastructures and its relation to National Security. This module provides an overview of the essential ideas that constitute the emerging discipline of Critical Infrastructure protection. It has two central objectives: to expand the way participants think, analyze and communicate about Critical Infrastructure security; and to assess knowledge in various sectors deemed as critical for National Security.

You will learn about the importance of Critical Infrastructure Protection, discuss about terrorism, crisis communication, conventional and unconventional cyber threats, weapons of mass cyber destruction, lessons learned from other nations and the role of NCIIPC.

Lessons:

- Introduction to Critical Infrastructure
- Role of NCIIPC
- Role of CERT-IN
- Policies to Protect Critical Infrastructure
- Readings
- Assignment
- Quiz

Week 2 – Smart Cities and Homeland Security of India

While India's internal security concerns may seem similar to those of other nations, India's geography – 7,000 km of coast and 15,000-kilometer land border – large population, social and political difficulties, dated security and scrutiny technological tools pose peculiar challenges.

Given the constraints, successive governments face a formidable task in identifying and containing security threats. The genesis of many terrorist movements has been internal.

The Ministry of Home Affairs has banned over 35 organizations around the country under The Unlawful Activities (Prevention) Act, 1967. Over the last few decades, the rise of terrorist groups in our neighboring countries has increasingly become a source of threat to our internal security.

In this module, we look at various internal security issues such as Naxalism and understand how such movements present the most significant overall threat to India. We will explore how technologies such as Drones, Artificial Intelligence, Face Recognition, Communications Intelligence and Surveillance solve multiple counter-terrorism challenges.

We will also cover smart city security from design and architecture perspective. The critical concepts of Crime Prevention through environment design (CPTED) will be discussed along with what every organization must do to enhance its physical security.

Lessons:

- Terrorism- External and Internal Threats to India
- Terrorism in the Digital Age
- Emerging technologies for Counter Terrorism Strategies
- Components of Smart City Security
- Water Security and Planning
- CPTED from an architecture perspective
- Physical Security strategies
- Readings
- Assignment
- Quiz

Week 3 – Economy and National Security

India is on a path to digitization and access to technology for its population. However, there are several challenges associated with the same. Campaigns like Digital India are beneficial to the masses and pose a massive problem for implementation, especially with limited resources and a developing economy.

Private Sector has played a pivotal role in the growth of almost every nation, and ours is no different. Ever since the regime of Globalization, Liberalization, and Privatization made headway in India, it has seen phenomenal growth. The Private Sector is also critical in securing a nation's security interests.

The cost of cyber-crime is another challenge that an economy faces. Even though it is tough to decipher, you will be surprised to witness how much the economy suffers due to online menace.

This Module will discuss and analyze all these aspects and how a nation can deal with such threats. In addition to this, we will look at cryptocurrencies and how a parallel economy can impact the National security.

Lessons:

- Digital Campaigns and Vulnerabilities
- Private Sector, Business Intelligence and National Security
- Cost of Cyber Crimes
- IPR Theft
- Cryptocurrencies
- Dark web
- Narcotics – Drugs online and economy
- schools and Institutions – What can be done
- How to drive awareness campaigns
- Readings
- Assignment
- Quiz

Week 4 – Electronic Contamination and Cyber Warfare

Cyberwarfare refers to politically motivated hacking to conduct sabotage and espionage. It is a form of information warfare sometimes seen as analogous to conventional war, and in 2013 was, for the first time, considered a more significant threat than Al Qaeda or terrorism by many U.S. intelligence officials.

In this module, we explore the various aspects of Cyberwarfare, Weapons used in cyberwar, economic warfare, the underground market of exploits, threats of electronic contamination, and its impact on National Security.

We will also discuss on Security Operations Center and how they can be effectively tested for maturity by Red Teaming with a hands-on lab activity.

Lessons:

- Methods of Hacking
- Darkweb Web
- Exploitation – Live Demo
- State Sponsored Cyber Terrorism
- Hacker Communities in India
- Maritime Cyber Security – importance for India
- Security Operations Center (SOC) and Enterprise Security
- Red Teaming – what it takes
- Hands-on: Defensive Cyber Operations
- Readings
- Assignment
- Quiz

Week 5 – Intelligence and National Security

Recent violent incursions in India by our neighbors have put the spotlight on National Security. This course examines key questions and issues facing the Indian intelligence community and its role in National and Internal security.

Delegates will have the opportunity to adequately address policy, organizational and substantive issues regarding homeland intelligence support. Course reference materials will provide an overview of diverse intelligence disciplines and how the intelligence community operates.

This module will look at Intelligence and National Security - the emphasis will be on issues affecting policy, oversight, and intelligence support to homeland defense/security and national decision-making.

Lessons:

- Need for Intelligence
- Open Source Intelligence
- Case Study- Pakistan Cyber Warfare
- Running a successful offensive cyber security operation
- Hand-on: Offensive Cyber operation
- Importance of Foreign Intelligence

- Bug bounty programs – How to utilize them effectively
- Running Responsible Disclosure programs
- Driving research communities in cyber security
- Incubation hubs for cyber security – key factors
- Readings
- Assignment
- Quiz

Week 6 – Digital Forensics, Legal System and Privacy Challenges in India

Cyberlaw is a generic term that refers to all the legal and regulatory aspects of the Internet and the World Wide Web. Anything concerned with or emanating from any legal aspects or issues concerning any activity of netizens and others in Cyberspace comes within Cyberlaw's ambit.

Privacy law refers to the rules that deal with the regulation of personal information about individuals collected by governments and other public and private organizations and their storage and use.

In this Module, we learn about the various laws in India related to Cyber and Privacy, with a particular focus on IT Act Law.

Lessons:

- Building Incident Response and Digital Forensic teams
- Emerging challenges in Forensics
- Cyber Insurance – what you need to know
- Legal Acts on Terrorism
- Maritime Law and Coastal Protection
- Cyber Laws and its Limitations
- Information Technology ACT 2000
- Readings
- Assignment
- Quiz

Week 7 – Artificial Intelligence and Machine learning

With every other product or technology claiming to be "enabled" with Artificial Intelligence, it is essential to know what AI realistically can and cannot do. We will explore the meaning behind common AI terminology, including neural networks, machine learning, deep learning, and data science, and learn how to spot opportunities to apply AI to problems in your organization.

In this module, we will learn about other emerging technologies and explore how you can drive capacity building in these so that your business is future-ready.

Lessons:

- Overview of AI and ML
- How to identify fake AI and ML technologies

- Putting Artificial Intelligence and Machine learning in practice
- Emerging technologies overview
- Building capacity in emerging technologies
- Managing centers of excellence
- Using next generation simulation programs
- Professional Ethics
- Case Study: Mission Reach
- Readings
- Assignment
- Quiz

Week 8 - Interaction with Government/Intelligence Agencies

As part of the program, all the delegates participating in the scholar program will get an opportunity to interact with various law enforcement and intelligence agencies in India. The sessions will allow the delegates to have a face to face discussion with leading officers from these departments and talk about the various challenges faced by the organizations in their goals of National and Homeland security.

Lessons:

- Interaction with CERT-IN
- Interaction with NCIIPC / NTRO
- Interaction with Law Enforcement Agencies

Annexure B

PAYMENT INFORMATION

Vendor Name	**INFORMATION SHARING AND ANALYSIS CENTER**
Address Line1	319A, LOGIX TECHNOVA, SECTOR 132, NOIDA
Address Line2	GAUTAM BUDDHA NAGAR, 201304
Email ID:-	support@isac.io
City	NOIDA
State	UTTAR PRADESH
Country	INDIA

Bank Name	**IndusInd Bank Ltd**
Bank Address	Preet Vihar, New Delhi Bank
Account Number	**259873869121**
IFSC Code	INDB0000031
Swift Code	INDBINBBDEP
IBAN Number	
Account Type	Current A/c

PAN Number	AACCI7629G
GST	09AACCI7629G1ZD

Please use the information on next page to reach us.

Reach us

INFORMATION SHARING AND ANALYSIS CENTER

For any further information, please reach us:

- Group Captain P Anand Naidu (Retd) – 8800880757 | pan@isac.io
- Dr. Amanish Lohan – 9813304226 | amanish@isac.io
- Rajshekhar P – 8527465252 | rajsm@isac.io

EMAIL US: support@isac.io

WEBSITE: https://www.isac.io | https://www.isacindia.org