**National Centre of Excellence**
for Cybersecurity Technology
Development & Entrepreneurship

DSCI PROMOTING DATA PROTECTION
A NASSCOM® Initiative

Ministry of Electronics & Information Technology
Government of India
सत्यमेव जयते

# Cybersecurity R&D Roadshow

## *POST EVENT REPORT*

06th NOV | 10:15 AM 05:45 PM

# CONTENTS

## Event Summary

National Centre of Excellence for Cyber Security Technology Development and Product Entrepreneurship, a joint initiative of Data Security Council of India (DSCI) and the Ministry of Electronics and Information Technology (MeitY), has hosted a Cybersecurity R&D roadshow to provide a platform to academia, research institutes and PSUs to exhibit their cybersecurity research, prototype, and products.

The virtual roadshow brought together key government stakeholders such as MeitY, NCSC, leading academic institutions like IIT Kanpur, IIT Kharagpur, IIT Jammu, IIT Delhi; user organizations like CDAC, BARC, CSIR, and multinational firms such as Crowstrike, IvyCap Ventures on the same platform.

An exhibition was hosted comprising 20 leading research projects in Cybersecurity by institutions like CDAC, BARC, IIT Jammu, IIT Roorkee, IIT Dhanbad BITS Pilani, IIT Kharagpur, among many others, to explore the Country's R&D Capabilities and current research projects. The various plenary and other sessions highlighted the multiplying efforts in cybersecurity research to make India a Global Hub for Security R&D and Product Entrepreneurship.

# Agenda


10:15 TO 11:00
Inaugural
Welcome Address
Keynote Address
11:00 TO 11:45
Plenary
Cybersecurity R&D: Scaling up for India's Future Readiness
11:45 TO 12:00
Presentation
Multiplying the efforts in Cybersecurity R&D
12:00 TO 13:00
Session
Explore the Country's R&D Capabilities & Work
Exhibition Time
12:00 TO 12:20
Next Generation Network Security
... BARC's R&D program in Electronics, Control, Instrumentation and Computers
12:20 – 12:45
Leading Public Sector Cybersecurity R&D Effort
... Cyber Security R&D of C-DAC
12:45 – 13:05
Leading Public Sector Cybersecurity R&D Effort
...Cyber Security R&D of CSIR
13:00 to 14:00
Wellness Break | Exhibition Time
14:00 TO 15:00
Sessions
Use Cases and Opportunities of Cyber Security R&D
... IoT/Hardware, Cloud, Quantum, 5G, Automotive, etc.
Cyber Collaboration: Industry, Start-up & Academia
... Case studies of how this has worked
15:00 TO 16:15
Session
Explore the Country's R&D Capabilities and current research projects
Exhibition Time
16:15 TO 16:30
Special Address
Role of Government in Fostering Cybersecurity RnD
16:30 TO 17:15
Session
Making India a Global Hub for Security R&D and Product Entrepreneurship
17:15 TO 17:45
Exhibition Time

## Session 1: Inaugural session


The cybersecurity R&D roadshow was kick-started by a warm welcome address by **Ms. Rama Vedashree, CEO, Data Security Council of India.** Rama emphasized how the Government and other industry sectors are leading technology adoption and the need to be cognizant of the underlying risks. She also stressed the importance of building its cybersecurity ecosystem, the cornerstone of indigenous intellectual property developed with continuous and sustained efforts. She emphasized how public-sector research labs like CDAC need to work collaboratively with private sector organizations, academia, start-ups, and large technology firms to commercialize their prototypes and offer solutions to the market. She re-iterated the need for a holistic approach to domestic research and development activities. While prototypes are being developed, they need to be aligned with industry use cases and built to be used commercially, thereby helping the country's overall cybersecurity landscape.


**Dr. Rajendra Kumar, Additional Secretary, MeitY,** while delivering his inaugural address, emphasized the importance of the cyber world and stated how the cybersecurity R&D roadshow was a testimony of the growth of the cyber world.Dr. Kumar reminisced about the Government's Digital India program, which was launched in 2015, and has systematically brought mainstream government functions as a part of the country's digital economy. He also focused on the importance of cybersecurity for digital interventions. He recognized that organizations' threats had grown many folds, especially during the pandemic, when the world has switched to virtual platforms. He revealed how the Ministry itself is pushing for a digital economy in India and targeting that digital enablement

contributes at least US $1 trillion in India's target of becoming a US $5 trillion economies by 2025. Dr. Kumar concluded his remarks by stating how the Government has set up advanced IT infrastructure labs in all states and focuses on capacity building in cybersecurity to tackle advanced level threats. With over 28000 police officers and 1000 officers from the judiciary already trained, the Government is gearing up to face the next wave of cyber threats and wants to enhance its cyberspace capabilities.

**As part of a special address, Dr. Rajesh Pant, National Cyber Security Coordinator, Government of India,** echoed our Honourable Prime Minister's call for self-reliance or Atma-nirbhar Bharat and mentioned that this equally applies to cybersecurity. He highlighted that even though some significant global organizations have large R&D centers located in India, India's overall recognition and contribution in the R&D space have not been significant. Dr. Pant emphasized that this paradox is due to challenges in translating research results and meaningful development in products and solutions. He highlighted how India's Government, via its projects, plans to establish a Center of Excellence in 25 technology-driven sectors. These CoE's shall be premier research institutes connected with academia and other research organizations and act as nodes by being further related to 500 start-ups across the country in the coming five years.

## Session 2: Cybersecurity R&D: Scaling up for India's Future-Readiness


## Session summary:

The discussion revolved around scaling up cybersecurity R&D to enhance the country's future-readiness and view the present landscape and the challenges that all stakeholders need to focus on.

India is already witnessing a surge in the number of reported cyber threats. The recent trend of organizations encouraging work from home is anticipated to increase cyber breach attempts. The panel stated that the experience gained from tackling sophisticated and

unique cyber incidents needs to be shared with researchers to aid indigenous products' development. Researchers in the country are already working on addressing use cases covering network security, cryptography, and threat intelligence; however, there is a vast untapped potential in the country as researchers are working in silos or local clusters. There is a need for collaborative effort across different government agencies (such as MEITY, DoT, and DRDO), industry bodies (DSCI), and academia.

The panel further deliberated on the convergence of Informational Technology (IT) and Operational Technologies (OT), giving rise to cyber-physical systems and developing adaptive trust models using AI/ML to protect such environments. To address security threats facing cyber-physical systems, SCADA testbeds are available in the country as test environments; however, there is a need to gain practical insights by partnering with MSMEs to iron out challenges and evolve use cases and develop new solutions. Globally, the research process is well defined to achieve tangible outcomes and solutions which can be monetized. Similarly, there is a need to establish an integrated national framework on funding product development to address different cybersecurity aspects, aided by an incubation ecosystem.

## Session 3: Multiplying the efforts in Cybersecurity R&D


### Session summary:

The National Centre of Excellence (National CoE), a joint initiative of DSCI and MEITY,has undertaken numerous initiatives to drive product entrepreneurship, given the importance of multiplying efforts in R&D through nurturing and attracting young talent with strong mathematical and analytical skills. The National CoE plans to utilize available R&D budgets to fund and develop deployable prototypes for enterprise security markets. The process of incentivizing start-ups and the need for product engineering skills that help scale up from pilot deployments were also presented during the session. The recent setup of a high computing facility by Nvidia and CDAC to encourage private investments in cybersecurity R&D is an example of public-private partnerships in this space. There is a need for greater industry involvement in R&D efforts through feedback, reviews, providing real-time use cases and datasets. The NCoE is working towards enabling this exchange and coordination between various stakeholders and partnering with the Indian IT industry to create a global reach for India's innovations.

## Session 4: Explore the country's R&D capabilities and work

0



## Session summary:

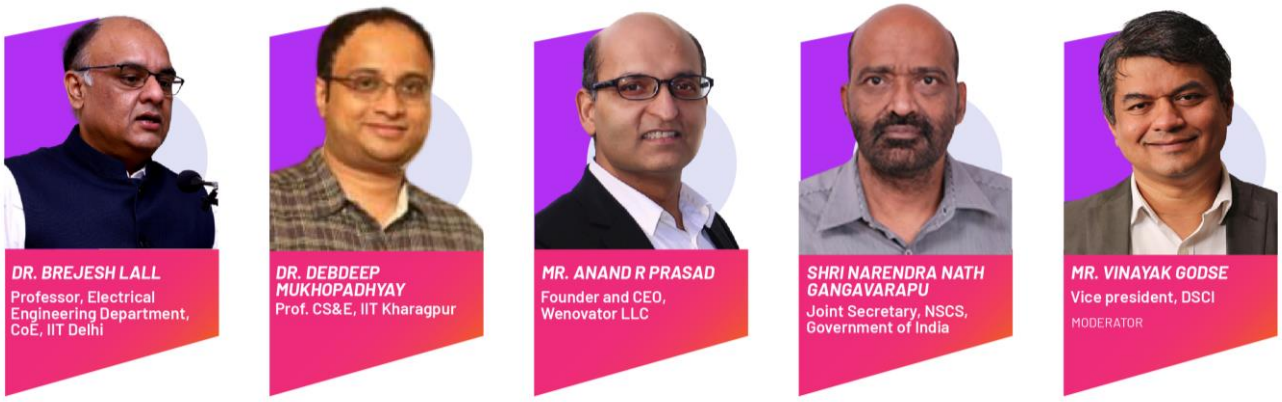
**Mr. Vinod Kumar Boppanna, Scientific Officer, Bhabha Atomic Research Centre**, introduced some of the next-generation security capabilities being developed by BARC's R&D program in the security of electronics, control, instrumentation, and computers. He also provided insights on on-going research programs being undertaken in cryptographic algorithm development, ransomware detection, big data analytics over network monitoring, and device security. He also shared updates about the Secure Network Access System (SNAS) network monitoring capabilities to identify network trends and behavioral anomaly detection in both applications and endpoints.

**Dr. Subramanian Neelakantan, Senior Director, C-DAC,** gave a brief about the National computing mission spearheaded by C-DAC through establishing supercomputing facilities and working on various indigenous technologies. He gave a short glimpse of multiple technologies being developed at C-DAC like Param Shavak, a High-Performance Computing system, automatic fare collection system, a telemedicine solution for the national digital health mission, NAADI ecosystem for covid-19 monitoring with on-field data from ASHA workers, and SAMHAR a healthcare analytics initiative for combating the current pandemic. He also elaborated on the cybersecurity R&D evolution at C-DAC and various solutions produced by them, including endpoint security, dynamic firewall, attack analysis, cryptography and PKI, and cloud security.

**Dr.Gopal Krishna Patra, Senior scientist, CSIR,** showcased a Darknet monitoring solution currently under development at CSIR and several research programs on cryptographic research for cyber-physical systems. His detailed presentation stories set up a first of its kind Vehicular Ad-hoc Network (VANET) testbed in the country. Dr. Patra also made a call for collaboration with industry partners in the planning, conceptualization, and execution of projects on intelligent systems.

## Session 5: Use cases and opportunities for Cybersecurity R&D

*... IoT/Hardware, Cloud, Quantum, 5G, Automotive, etc.*




## Session summary:

The discussion revolved around building the nation's strategy to scale up R&D for cybersecurity. On the one hand, there are constraints on the research cases available to the community. On the other hand, there are challenges related to scaling up existing R&D efforts in the country.

The panel considered various emerging scenarios, describing the evolution and expansion around applications and networks and the corresponding need for cybersecurity solutions to evolve. As IoT proliferates, the associated vulnerabilities and related threats can bring disastrous effects on the organization's security and cause ripples in the country's cybersecurity fabric. Thus, there isa need to incorporate security by design. However, developers and engineers are not security experts, and therefore, foundational elements of security are routinely overlooked even though the industry recognizes the importance of building secure products and services. Audit programs are currently used as a lever to measure gaps and elevate protection for an organization. During each audit cycle, known vulnerabilities are routinely rediscovered. Yet, retrofitting security because of audit findings is not the best approach. Underlying fundamentals of security remain constant while technology will evolve. Organizations realize that the next wave of growth can only be driven with security being leveraged as an enabler and a business driver.

Cybersecurity is multi-dimensional; we need to focus on data security, device security, and user security. The panellists emphasized how ensuring security by design should be a significant focus area for India's research community. Value creation in cybersecurity research can be achieved by devising a strategy that involves prioritizing initiatives, formulating partnerships, and identifying necessary catalysts. A constant dialogue around the emerging methods and challenges is required, along with a periodic review of work being undertaken at the national or local level, to elevate its research capability. There is a need to ensure that the curriculum taught in various engineering institutes and labs connects with actual industry problems. There is also a need for imbibing lessons from research on social

sciences and policymaking to tackle blind spots being created for the evolution of cybersecurity capability.

The research and engineering gap can be tackled through incentivization, where solution engineering is rewarded. Setting up specialized centers such as the one at CDAC for areas like hardware security increase the work's visibility and highlight various personnel's expertise. Connecting researchers' ecosystem with start-ups and industry is essential, and efforts to enable the same need to be undertaken nationally. Another way to achieve this is by having longer-term research plans for various stages of the research and engineering cycle,planning for outcomes to reap benefits in the next 10-15 years, thereby helping achieve longer-term strategic goals.

## Session 6: Special keynote on India's cybersecurity R&D


**Mr. Ajay Prakash Sawhney, Secretary, MeitY,**in his special keynote on India's cybersecurity landscape, emphasized that Research and Development, along with product development, are needed for a cyber-secure nation. Mr. Sawhney indicated how a dedicated group in MEITY works with premier educational institutes and industry bodies to shape cyberspace activities. He lauded the role of CDAC and STQC in looking at new threats and developing strategies with regards to combatting emerging threats. He acknowledged that the National Centre of Excellence, setup with the help of DSCI, has helped in providing the necessary impetus to Research and Development and developing and designing an overall growth strategy for the cybersecurity ecosystem in the country. He also drew on the participants to ponder upcoming technology such as 5G, which shall open new research and development opportunities in cyberspace. Mr. Sawhney also expressed concern about the vulnerabilities surrounding the Internet of Things, one of the many technologies that will increase once 5G is rolled out. He mentioned how hardware-level threats (embedded in devices) could be significant threat vectors in the nation's mission-critical sectors. He reflected on issues due to inroads (encroachments) made into personal data privacy because of security challenges related to the trusted value chain/supply chain of technology. Mr. Sawhney also elaborated on the Government's approach in encouraging indigenous R&D output to be deployed within the Government's ecosystem, thereby creating an opportunity for Public-Private Partnership (PPP) Cybersecurity. He concluded his remarks by stating the importance of team efforts at a

national level – a team comprising local talent and stakeholders' actions from the Government, industry, and academia.

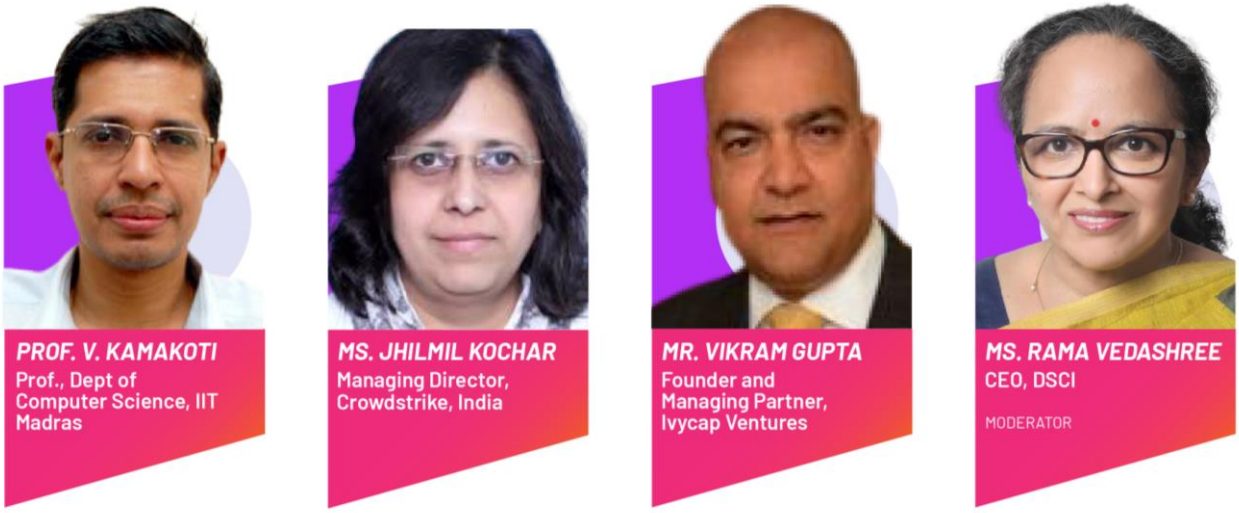
## Session 7: Explore the country's R&D capabilities and current research projects.

**Prof. (Dr) P. Sateesh Kumar, Associate professor, Computer Science and Engineering, IIT Roorkee,** focussed on IIT Roorkee's hybrid detection model combining permissions and traffic features for an Android malware detection system. He elaborated on how it shall use a two-phase hybrid detection system and Fp growth frequent patterns to generate and analyse results. KNN algorithms, coupled with a combination of unsupervised leanings, K- medoids learning, and supervised KNN, shall help achieve a better decision rate rather than only using KNN and helping researchers evolve use cases cybersecurity applications.

**Prof. (Dr) Deepak Garg, HOD and Professor, Computer Science Engineering, Bennett University,** spoke about how Bennett University is working with Industry partners like NVIDIA, CISCO, DSCI, etc., are soon to launch a B.E. course in Computer Science with a focus on Cybersecurity. He gave a brief on a few projects undertaken at the university; namely, HT-Pred, which is a defensive machine learning tool for hardware Trojan detection, the Security assessment in IoT network using traffic statistics, IoT network traffic classification & AI - Intrusion Detection System using ML, click fraud detection for click-through rate, violent action recognition using surveillance, development of lightweight image encryption technology for cloud-enabled IoT applications using chaotic systems and DNA based authentication protocols for securing resource-limited mobile environments**.** He also spoke about a defensive machine learning tool for hardware Trojan detection and security assessment in IoT networks, which was developed to analyze traffic through splitting feature extraction and flow construction. Dr. Garg revealed that the university conducted workshops on cybersecurity, which covered 15,000 educators, thereby reaching approximately one million students during the Covid-19 pandemic period. Dr. Garg also pointed out that the companies that are spending billions of dollars in marketing budgets are susceptible to frauds and proxy clicks. The university hopes to provide a viable solution in this space.

**Prof. (Dr) Gaurav Varshney, Assistant Professor, Computer Science and Engineering, IIT Jammu,** divulged that they develop an access control and authentication prototype. He explained how the institute wishes to establish a facility for one-time use cards and former card that works on offline authentication, card cloning, and developing touchless authentication. With the help of the on-demand generation of payment cards, the user will generate his card at the click of a button, thereby eliminating card cloning. The institute is also integrating touchless authentication for banking to secure and spoof proof to ensure that the leaked data will not be identifiable. They wish to develop a trusted payment system and solve the problem of varying trust. They aim to build privacy-preserving models, avoid brute force attacks, generate cards that are easy to use, and achieve card protection using QR codes.

## Session 8: Making India a global hub for security R&D and product entrepreneurship.

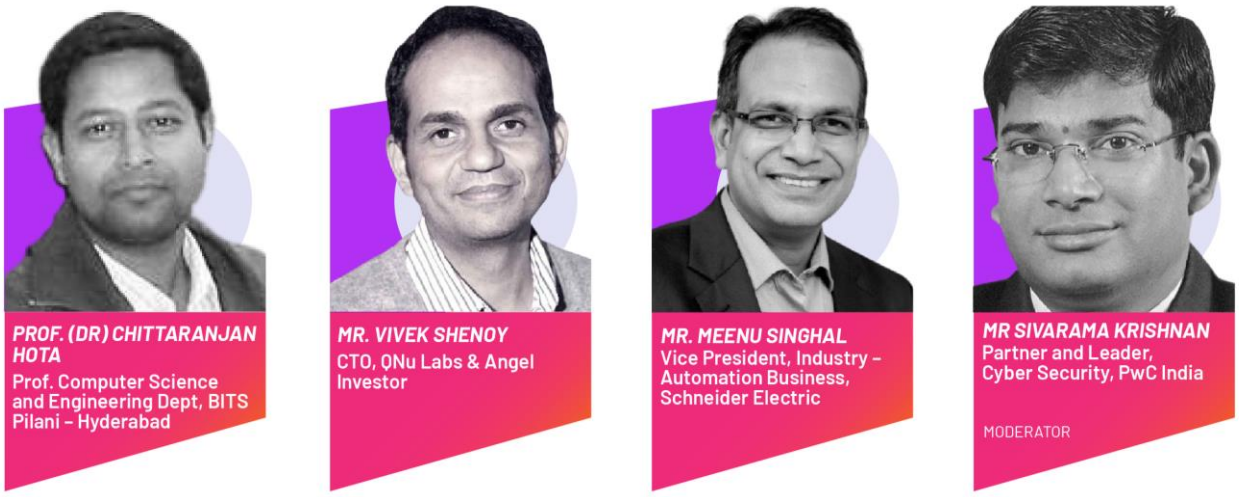



## Session summary:

In the last session of the event, the focus was on 'Making India a Global Hub for Security R&D and product entrepreneurship. 'Both NASSCOM and DSCI drive the agenda of making India a global hub for Cybersecurity R&D and growing the industry US $30 billion by 2035. The panel agreed that this growth could be sustained by focusing on strengthening cybersecurity ecosystems to benefit from adopting digital technology.

To achieve this milestone, there is a need for Government, Academia, and Industry to prepare a roadmap for driving Cybersecurity R&D in the nation. There is also an urgent need for capacity building in the field of Cybersecurity R&D and covering gaps for investments made in boosting R&D activity in the country. Further, global institutions need to be approached for forging a partnership with academia, and endowment funds need to be set up to facilitate research and innovation. The focus on building sustainable innovation programs and the importance of co-creation, like the model followed by FinTech companies, were emphasized in the session. Four key focus areas in research covered during the discussion were - *Gathering threat intelligence, Managed threat hunting, Forensics, and Incident Response and Endpoint protection through the latest technologies like AI*.

## Session 9: Cyber collaboration: Industry, Start-up & Academia



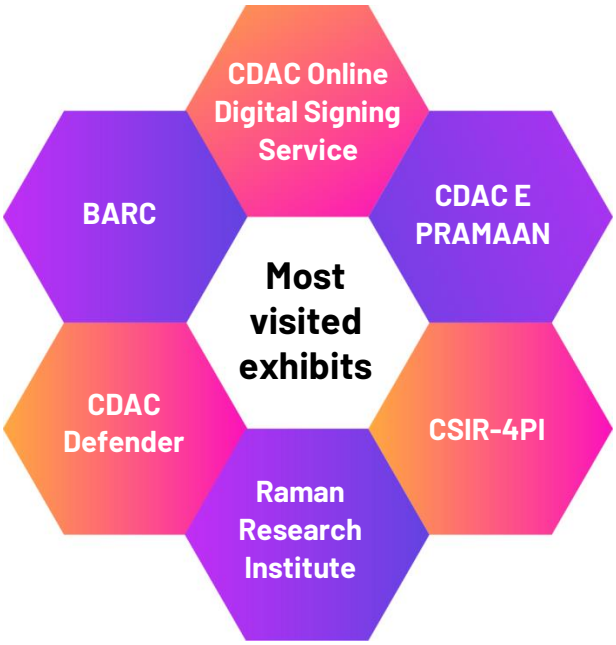

## Session summary:

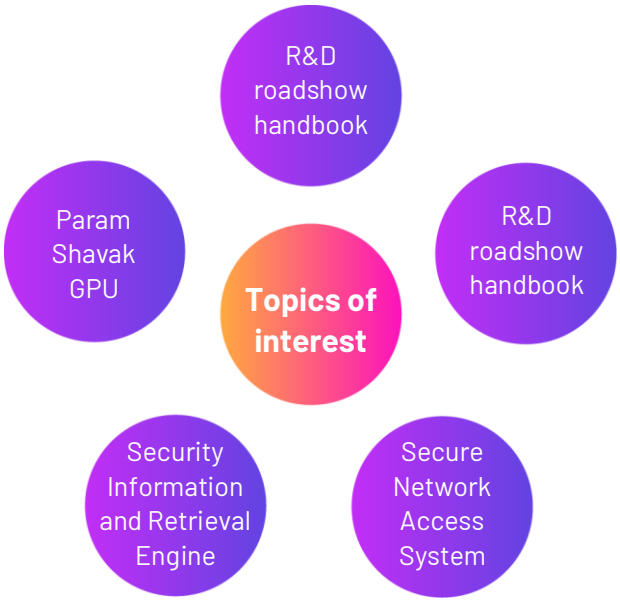
In this panel discussion, the relevance and importance of 'Cyber collaboration: Industry, Start-up & Academia' were deliberated in depth. For the cybersecurity industry to grow, ideas from academia need to be funnelled to start-ups for developing products and, consequently, scaled up through their effort. The panelists discussed the current state of research undertaken by academia and the importance of using an approach that focuses on bringing forward ideas that can be developed into products. This requires a paradigm shift in academia and needs to be imbibed across institutes, including premier academic institutions in India. Given the importance of innovation being driven through academia, the industry must extend its support to credible ideas from academia and start-ups.

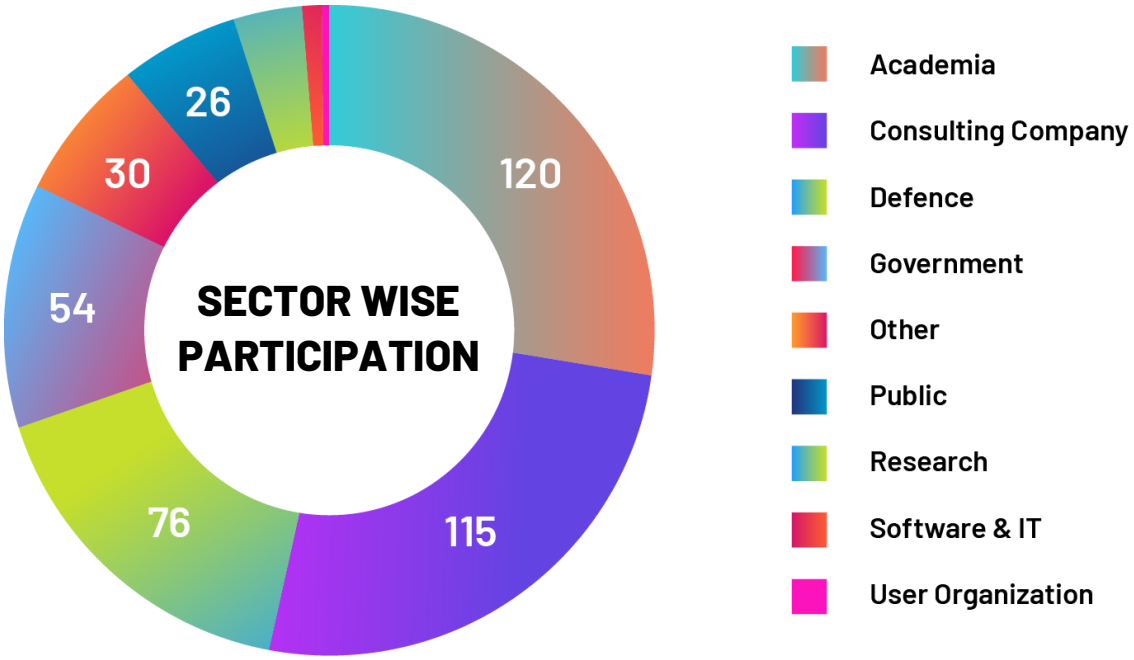
Further, to make the environment conducive to the growth and adoption of such ideas, the ecosystem needs to be bolstered with incubation centers and test labs. The talk highlighted the need for an integrated listing of all labs and test equipment available across India to better access researchers. The panel agreed that academia is changing and are trying to balance themselves and highlighted their need for access to funds.

## Event Statistics

| Registrations | Exhibitors | Speakers | Total downloads |
|---|---|---|---|
| 915 | 20 | 24 | 1008 |

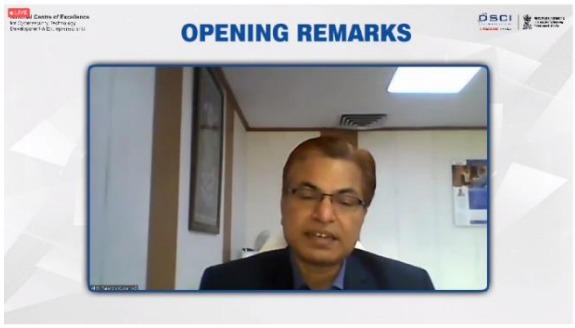


# Events Gallery













## Get in touch with us

**Address** : 3rd Floor, NASSCOM Campus, Plot No. 7-10, Sector 126, Noida, UP -201303
**Email** : ncoe@dsci.in **Contact** : +91 2598 987451