**Roundtable Session on Cyber Defence Resourcing "A National Priority"
by Cyber Vidyapeeth Foundation**

Date & Time: 23rd May, 2022

        Session 1: 11:00 AM to 1:00 PM

        Session 2: 2:00 PM to 4:00 PM

Organizer: Haryana State Higher Education Council (HSHEC)

Location: Conference Hall, HSHEC, Panchkula

Agenda: Challenges and Opportunities related to Cyber Defence.

Steps needed for Cyber Defence education in next 10 year in Haryana.

Cyber defence opportunities in India and role of Haryana.

Present:

1. Sh. Shashank Shekhar Garuryar, Chairman, Cyber Vidyapeeth
2. Sh. Balaji Venketeshwar, Chief-Mentor, Cyber Vidyapeeth
3. Sh. Arvind Tripathi, Member, Cyber Vidyapeeth
4. Sh. R.V.S. Mani, Member, Cyber Vidyapeeth
5. Dr. Rajendra Nath, Chairman, Department of Computer Science and Applications, Kurukshetra University, Kurukshetra
6. Dr. Ashwani Kush, Director, IT Cell, Kurukshetra University, Kurukshetra
7. Dr. Dhiraj Khurana, Assistant Professor, Maharshi Dayanand University, Rohtak
8. Dr. G.P. Sardha, Director, University Computer Center, Maharshi Dayanand University, Rohtak
9. Dr. Digvijay Singh Sharma, Information Security Officer, Maharshi Dayanand University, Rohtak
10. Prof. Ajit Singh, Dean Academic Affairs, and Head of Department, CSE/IT, Bhagat Phool Singh Mahila Vishwavidyalaya, Khanpur Kalan, Sonepat
11. Dr. Pradeep Kumar, Dean Academic Affairs, Dr. B.R. Ambedkar National Law University, Sonepat
12. Mr. Chandan Adhikari, Incharge IT, Dr. B.R. Ambedkar National Law University, Sonepat
13. Dr. Manju Pruthi, Dean Academic Affairs, Indira Gandhi University, Meerpur
14. Prof. Savita Sheoran, Chairperson and Dean, Department of CSE, Indira Gandhi University, Meerpur
15. Dr. Anupam Bhatia, Deputy Controller of Examination, Chaudhary Ranbir Singh University, Jind
16. Dr. Amit Kumar, Incharge UCIC, Chaudhary Ranbir Singh University, Jind
17. Dr. R.K. Gupta, Dean Academic Affairs, Chaudhary Bansi Lal University, Bhiwani
18. Prof. Dinesh Kumar Madan, Chairperson, Department of ICT, Chaudhary Bansi Lal University, Bhiwani
19. Sh. Sahil Kukreja, Asst. Professor, Department of ICT, Chaudhary Bansi Lal University, Bhiwani
20. Dr. Amarpreet Kaur, Dean Academic Affairs, Gurugram University, Gurugram
21. Ms. Mahima, Head of IT, Gurugram University, Gurugram
22. Dr. Ravi Bhushan, Deputy Registrar, Maharishi Valmiki Sanskrit University, Kaithal

23. Dr. Shasshikant Tiwari, Head of Department, Department of Darshan, Maharishi Valmiki Sanskrit University, Kaithal
24. Prof. Harbhajan Bansal, Dean Academic Affairs, Guru Jambheshwar University of Science & Technology, Hisar
25. Prof. Dharmendra Kumar, Chairman, Department of CSE, Guru Jambheshwar University of Science & Technology, Hisar
26. Dr. Ashutosh Dixit, Dean Academic Affairs, J.C. Bose University, Faridabad
27. Dr. Atul Mishra, Chairperson, Department of CE, J.C. Bose University, Faridabad
28. Dr. C.K. Nagpal, Professor, Department of CE, J.C. Bose University, Faridabad
29. Prof. Jyoti Rana, Dean Academic Affairs, Shri Vishwakarma Skill University, Palwal
30. Dr. Ravinder Kumar, Skill Associate Professor, Shri Vishwakarma Skill University, Palwal
31. Dr. Nitin Goyal, Skill Assistant Professor, Shri Vishwakarma Skill University, Palwal
32. Dr. Alok Srivastav, Professor, Department of Chemistry, Panjab University, Chandigarh
33. Dr. Bhoopesh Singh Bhati, Associate Professor, Chandigarh University, Mohali
34. Dr. Rakesh Sahu, Assistant Professor, Chandigarh University, Mohali
35. Sh. K.K Agnihotri, Advisor, HSHEC
36. Smt. Radhika Prajapati, Junior Academic Analyst and Planner, HSHEC
37. Sh. Apoorv Pandey, Junior Academic Analyst and Planner, HSHEC
38. Dr. Amarendra Kumar Aarya, Assistant Professor, HSHEC
39. Sh. Rajesh Kumar, Superintendent, HSHEC
40. Sh. Manjeet Singh, PGT Computer Science, HSHEC
41. Ms. Diksha Gupta, DEO, HSHEC
42. Mr. Manish Bisht, DEO cum Office Secretary, HSHEC

Representatives from the following Universities were not present:

1. Chaudhary Devi Lal University, Sirsa
2. Pandit Lakhmi Chand State University of Performing and Visual Arts, Rohtak
3. Deenbandhu Chhotu Ram University of Science and Technology, Sonepat

Topics discussed:

- Summarization of Ukraine Russia Asymmetric War
- Lesson learnt from current Cyber Flare
- Importance of cyber defence education & training
- Alarming cyber resource gap – statistics
- Mulling over resourcing problem and possible solution
- Industry resource need and cyber competency
- Haryana as key enabler for cyber resourcing
- Role of academia in cyber resourcing capacity building
- Cyber defence education Roadmap

Ms. Radhika Prajapati welcomed team from Cyber Vidyapeeth and the participants.

Sh. K.K. Agnihotri in his opening remarks said that the Chairperson after earlier interactions with the team from Cyber Vidyapeeth desired that there is a need to share the concept with the state universities, hence, this meeting has been organized.

Sh. Balaji Venketeshwar, Chief-Mentor, Cyber Vidyapeeth

The scope of cyber defence is too wide and difficult to be bound in a syllabus as it changes every day with every new cyber-attack.

Examples of cyber-attacks on critical facilities around the globe affecting many lives, like Malfunctioning missiles in Russia Ukraine Crisis, Collapse of phone network in Tunisia, Collapse of Russian Train systems, Collapsing power grids in Ukraine, Russia, and India.

Cyber-attacks impact all aspects of the value chain.

- o Disruptions/challenges for industry 4.0:
- o Cyber world is connected and asymmetric.
- o Hacking and cyber-attacks on daily basis.
- o Insider threats.
- o Online frauds due to unawareness and negligence.
- o Creating awareness for Cyber defence education.

Cyber Vidyapeeth is offering new syllabus for cyber defence but there are no takers for the course. Cyber defence is a full-fledged engineering science however, not currently not being considered as one.

It is estimated that India needs 3.5 million cyber defence engineers talent resource by 2026 and Cyber Vidyapeeth has committed to create 1 million cyber defence engineer, and India needs to take steps for it in the next 2 years. Till now Cyber Vidyapeeth has created 5,400 cyber defence engineers.

Focus on creation of Cyber Rakshak, Cyber Defence Research & Development, Cyber Defence discussion and discourse.

India should prepare for industrial revolution 4.0 which is cyber-physical systems in connected World.

John Hopkins Institute's research found Veda's contribution in industrial revolution by teaching self-sustainable production. India needs to create its own cyber defence jobs with indigenous consultancy firms.

Delhi reported 1600 crore cyber-fraud in last 9 months, Mumbai reported 2400 crore cyber-fraud in last 12 months. It is Important to spread cyber defence awareness for the users and for the authorities to report cyber fraud cases.

Benefits and possible applications of cyber defence:

- o Robot assisted production

- Predictive maintenance
- Additive manufacturing of complex parts
- Machines as service
- Big data drive quality control
- Production line simulation
- Smart supply network

India creates around 50 lakh IT and allied fields graduates every year, we need contribution from the higher educational institutions to prepare students for cyber defence education. For e.g. students can create indigenous countermeasures for cyber threats, for which we need to motivate the students for out of box thinking.

There are two aspects of cyber defence:

- Cyber Threats – Attacks which are done remotely by hackers.
- Insider Threats – Cyber security compromises due to unawareness of personnel working in the target organization.

Government of India has a project for Cyber defence, providing Rs. 10 crore funds to the institute that wants to take up the project.

Session 2

Sh. Balaji Venketeshwar, Chief-Mentor, Cyber Vidyapeeth

Elaborated with examples of the ways cyber-attackers can hack into our systems and inflict damage or collapse critical facilities. India is having an edge over China's cyber defence engineers due to better reputation.

Layered structure approach for Cyber defence education:

1. Cyber Security For All – Awareness – General do's and don'ts awareness (20 hours course for students in all streams).
2. Cyber Security Modules – Training – Specialization and project in one of the 27 Cyber security heads (6 months).
3. Cyber Security Electives – Education – Offering specialization in one of the 27 Cyber security heads as an elective in extensive courses (1 year)
4. Cyber Security Majors – Education – Offering extensive course in cyber security (1 year or more)

The specialization in cyber defence is much needed to be able to have talent resource in different aspects of cyber defence like psychology, law, statistics, mathematics, biotechnology, etc. who will be able to identify cyber defence risks in different fields.

Syllabus revamping is needed for including, for e.g. understanding cyber-physical dimension, embedding cyber learning in multi-disciplinary education, mass consciousness control, in the courses.

The cyber defence courses course curriculum are designed based on NEP 2020.

Strategies for India's Leadership in Cyber Education:

Rapid introduction of AICTE Model curriculum of courses at UG Level in Cyber Defence in all Technical College by May 2022.

- Training of all 9000+ Lecturers in IT/Computer Science in next 6 months in deep skill in Cyber Defence for early adoption of the Syllabus.
- Rapid Training in Cyber Defence 4 months course now covering around 2 lakh student of 30 lakh can be game changer next year.
- Trained trainer can work on PG level students from next year and produce 20,000 more next 2 year.

As knowledge of cyber defence is like a double edged sword, it can be used for defence as well as offence, tools will need to be used for ethical screening of students to detect anomalous characters before enrollment for advanced courses.

This will also go a long way in meeting the shortage of cyber defence man power nationally and also globally.

Mentoring to be provided to the teachers for first 2 years, during with they will build the capability of the teachers on cyber defence course and be self-reliant from 3rd year.

Discussions

Cyber Vidyapeeth may explore the scope of offering the courses to existing workforce in executive programs and continuing education programs.

No fees will be charged for MoUs, they may provide the open to all, free resources to the institutes, however, there may be some operational fees related content hosting.

Cyber Vidyapeeth would facilitate establishment of Center of Excellence in Cyber Defence in Haryana which would attract companies in the relevant domains and Haryana can carve a niche at national and international level in Cyber Defence.

Cyber Vidyapeeth will need atleast 5,000-10,000 students from 1 stream to offer a viable course.

Cyber Vidyapeeth already has 15 courses with specialized objectives.

Free for all open source content for cyber defence awareness consisting of general do's and don'ts to be shared with the institutions.

May look into possibility for training on Cyber Security for the teachers, a 40 day training course (20 days classes, 6 months for practice, 20 days classes) which provides 6 month access to online simulator.

NPTEL courses are more theoretical, Cyber Vidyapeeth provides project for the students to practice from real life examples.

Networking needs to be done with education system, consideration of AICTE on the Cyber defence syllabus.

For short term courses: No approval is required from statutory bodies for introducing such courses in alignment with the existing subjects for a duration less than one year at the universities.

The universities may plan roadmap for introducing specific courses with durations as shared through the presentation, training of faculty for inbuilt capacity in consultation and with nominal price, to be negotiated with Cyber Vidyapeeth by signing MoU or as may be required.

The meeting ended with a vote of thanks by Dr. Amarendra Kumar Aarya.