

CYBER PEACE CENTER OF EXCELLENCE



Cyber Peace
Foundation



“

INFORMATION BROCHURE

Cyber Security is a centre stage in our lives, but we continue to overlook the threat posed to national and individual security putting ourselves into peril. Over the years analysts and officials in government, and outside, have talked about the shortage of capability and capacity but the efforts to address these issues are found to be wanting, in terms of commitment, resource allocation and effort. While we laud the leadership of other countries in the domain, praise their skill incubators and seek partnerships, our own national effort for skill building, using the same models, is yet to be put into operations.

India has the largest number of educated youth and every year thousands are passing out of our Universities looking at joining the national workforce. The human resource is unmatched, in skill or numbers, and millions have migrated to the west to contribute to the success and growth of their enterprises and governments. Migration is (usually) on top of the minds of these young adults, and India is poorer for it.

Cyber Peace Center of Excellence seeks to explore a plan to harness the talent pool from among the youth through the participation of academic institutions, through programs to nurture innovations. Programs which will throw up challenges to institutions, their students and faculty, to work closely with government, law enforcement agencies and armed forces, taking up research and development programs addressing use cases provided by them.

About Cyber Peace Center of Excellence

A community driven collaborative technology research and innovation framework for academia. The idea is to harness the potential of young talent to research and innovate on potential areas of technical solutions. Being a collaborative platform the Industry, Government and other entities can share their problem statements and contribute towards innovative product and services.

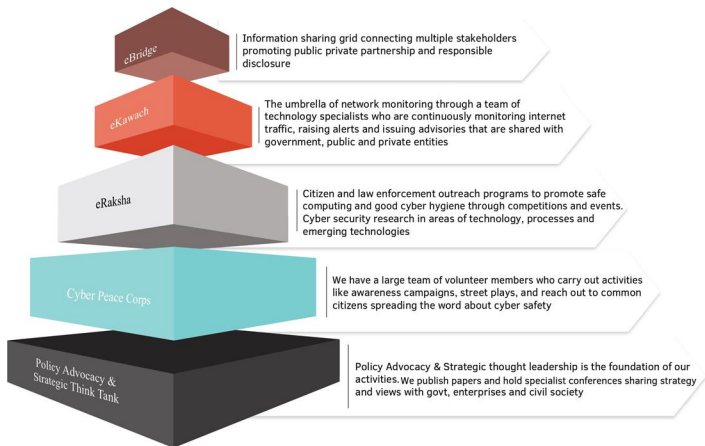
Academic Solution

Our academic institutions nurture millions of talented youth who carry tons of ideas in their minds, and the ambition, and will, to achieve their goals. This solution proposes to challenge the mind and talent of the students, mentored by the faculty in these academic institutions, The government establishment(s) has to partner with one or more academic institution, and share details about their operational challenges, issues, threats, risks and fears.

The institution takes up the real-life use case as a research and development project and develops a solution. Depending on the project, the IP for the solution can be licensed for commercial exploitation or handed over in national interest. Benefits accrue from this arrangement for all stakeholders:



Our youth are not adequately challenged, in opportunity and intellect, during the formative years in University, and they look to the west for fulfilment.



Cyber Peace Center - ongoing projects

Cyber Peace | Projects

Show 5 entries

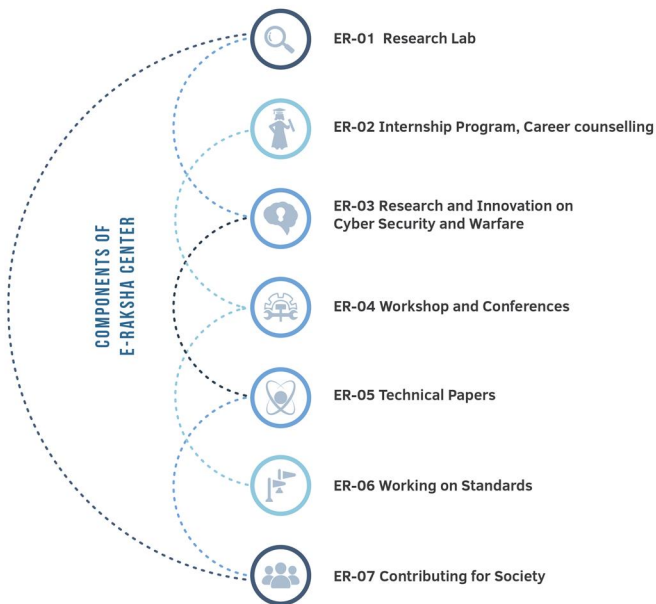
Project Name -	Description -	URL -	Project Leader -	Nodal Center -	Working Group -
E-Kawach	Early Warning System	VISIT WEBSITE	Dinesh Bareja	Cyber Peace Foundation - Research Wing	Honeyynet
Latency Mesurment	A tool to measure network latency	VISIT WEBSITE	Anand Raje	University of Petroleum and Energy Studies, Dehradun	Internet Routing and Peering
NCPCI Mobile App	Developing a Cyber Security Mobile app for kids		Sasank Borua	Royal Global University	Mobile Apps
Open CTF Platform	Building an open CTF platform		Mr. Jayesh M. Thakur	Veer mata Jijabai Technological Institute, VITI - Mumbai	Honeyynet
Trust Associated Library - Fake Identities and Content	A project to deal with fake news and entities on social media platforms		Vishal Kaushik	University of Petroleum and Energy Studies, Dehradun	Trust Associated Library



Existing Cyber Peace Center of Excellence

BIT, Meerut (UP) | UEM, Kolkata (WB) | Kaziranga University, Jorhat (Assam) | Veermata Jijabai Technological Institute, Mumbai (MH) | University of Petroleum and Energy Studies, Dehradun (Uttarakhand) | Government Engineering College, Bikaner (Rajasthan) | UEM, Jaipur | ICFAI University, Ranchi | Royal Global University, Guwahati | NIT Manipur | Indira Gandhi Delhi Technical University for Women | Redteam Hackers Academy, Kerala | Ansal University, Gurugram | Gujarat Technological University





ER-01 : Research Lab

The research lab envisions to foster community driven research on the following areas, the list is not exhaustive and will add more areas of research from cyber security and warfare domain.

- Research and analysis of the cyber security issues and threats such as botnet etc.
- Setting up malware analysis test bed and research and analysis of malwares.
- Setting up of a Honey Network & Hardware Security Test bed.
- Setting up of the cyber security simulation lab.
- Setting up of the critical information infrastructure protection lab.
- Setting up of IoT and smart city lab.
- Setting up DNS/DNSSEC testbed
- Setting up Internet DNS Traffic probe infrastructure
- Setting up of IoT, IPv6 and smart city lab.
- Setting of Internet Operations and Peering simulation lab



The Requirement (From Hosting Institutions)

Providing space (min. 900 sq. ft.) at a suitable location in the hosting institution to set up the research center and the lab/s associated with it.

Providing the space for training for the capacity building activities.

Providing the well-equipped space for the purpose of meetings and discussions as and when required. Hosting institution will remain the owner of this space.

Provide the well-equipped office space for the various officials/ guests/ experts of CPF visiting the research center or the university. Hosting institution will remain the owner of this space.

IT infrastructure to start the functioning of the research center. The minimum basic is listed as below -

Two Server with at least 32 GB RAM and 4 TB of Hard Drive.

20 MBPS Dedicated Static IP Internet link (separate from the routine institution link). Minimum /24 IPv4 and /48 IPv6 address pool with ASN number for Internet engineering research and development.

5 Raspberry Pi 3 with 16 GB UHS 3 MMC Card (64 GB).

5 Desktop Computers with high configuration (i5, 8GB 500GB)

UTM firewalls switches etc.



ER-02 : Internship Program, Career counselling

Internship

Internship program is crucial component of Cyber Peace Center and seeks to identify young ignited minds to work of research and innovations. The internship programs provide requisite exposure to real-life challenges and also involves careers cancelling for future.

There are good options of research after undergraduate levels and this program provides the requisite content to foster the culture of research driven academic environment.

Note : The Internships are for selected talented students based on tests and other criteria set by CPF time-to-time.



ER-03 : Research and Innovation on Cyber Security and Warfare

This component aims at bringing Cyber Security and Warfare problem statements and research scopes to the academia. The core objective of setting up E-Raksha initiative largely depends on this component where different stakeholders collaborate to solve real life situations and young ignited minds start taking interest in ground breaking research initiatives for real life cyber security risks and threats



ER-04 : Workshop and Conferences

The workshops and conferences for faculties and students will help in building capacities on Cyber Security and Warfare technologies and research areas . Seeks to improve the required skills and capabilities of the young talent to explore innovative ideas.

The workshop will be in collaboration with Industry, Government and other entities and will provide a platform to engage in dialogue with experts in the filed.



ER-05 : Technical Papers

One of the major areas of improvement in building research and innovation mind set among the young brains is to express their ideas and accomplishments in different platforms and building the skills to write technical papers. This exposure will help many ideas to nurture and also help in building reputation of the institution.

This component will help grow technical paper writing skills and also collaborate with and build platforms where the students and faculties can showcase their ideas and get peer reviews. One such initiative is 'Cyber Peace Journal' and the students and faculties are encouraged to send their entries for its different additions.

More details at : cyberpeace.world



ER-06 : Working on Standards

India's contribution towards Internet standards is poor and with the 'Digital India' being the next generation India, its high time our young talent start developing protocols and standards for the next Generation Internet, which the world will use.

Cyber Peace has partnered with organizations to provide the platform to Cyber Peace centers, starting working on standards.



भारतीय मानक ब्यूरो
Bureau of Indian Standards
The National Standards Body of India

ER : 07 Contributing for Society

Young minds actively participating in technical community problem statements helping in cyber crime issues, working with the neighborhood.

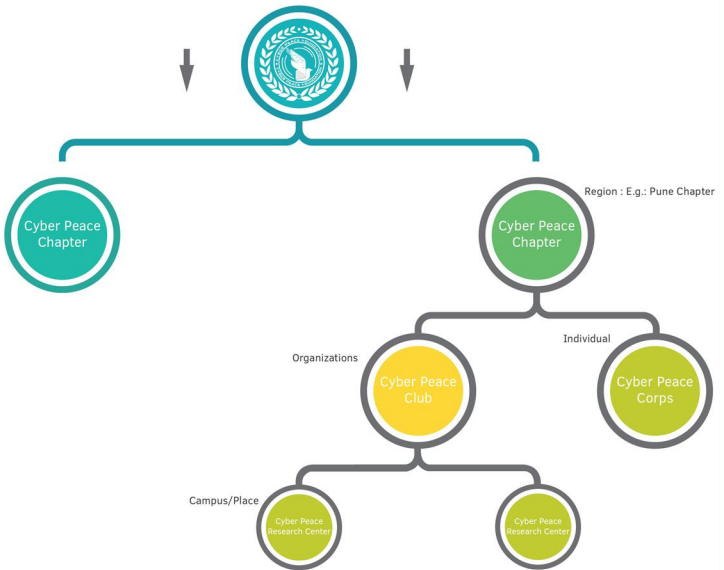
Cyber Peace Corps – one of the initiatives of CPF envisions to develop a link between talented brains and the society to curb cyber crime. The students and faculties E-Raksha initiative in the campus can be of great help in building a community chain to fight against cyber crime. This component seeks to engage young minds to start working on innovative ideas for cyber security at the ground level.



Cyber Peace Lifecycle

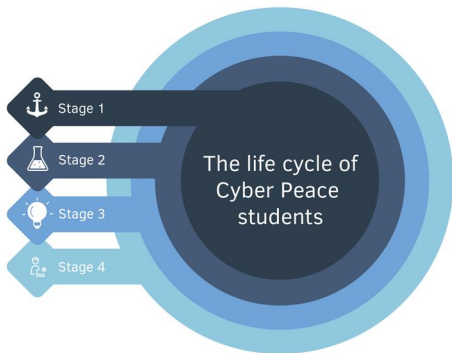
How Cyber Peace Works?

THE GOVERNANCE FRAMEWORK



The life cycle of Cyber Peace students

- **Year 1**
Incubate & Learn
- **Year 2**
Engineer
- **Year 3**
Innovate
- **Experts**



The idea is to build an innovation ecosystem in the campus. The students of Cyber Peace will be contributing in their entire lifetime. Students will be enrolled every year for Cyber Peace center through a competitive process.

Incubation : Year 1 : Interested students will be enrolled. The focus will be more on building the infrastructure, capacity building and establishing a tightly coupled team.

Engineering : Year 2 : The focus will be more on problem solving and working towards real life cyber security challenges. 2nd year students will mentor 1st year

Innovation : Year 3 : The team will innovate, technical papers, standards, startups, research will be core focus. 3rd year students will mentor 2nd year

Experts : Alumni students will be Cyber Peace experts



Y1 : Incubation

ER-01	ER-02	ER-03	ER-04	ER-05	ER-06	ER-07
Setting Up the Lab	Summer Internship	Cyber Security project	(01) Free Beginners Cyber Security Workshop	(12) Technical blog	Indian IETF Capacity Building Program	Forming a Cyber Peace Corps unit in campus
	Winter Internship	Global Cyber Challenge	(02) Paid Beginners Workshop	(03) Technical Research Papers	Open Source Implementation	Engaging in CPC activities

Y2 : Engineer

ER-01	ER-02	ER-03	ER-04	ER-05	ER-06	ER-07
Setting up Advanced Lab	Summer Internship	Cyber Security Projects	(01) Free Advanced Cyber Security Workshop	(12) Technical Blogs for publication	W3C Standards	Engaging in Cyber Peace Corps activities worldwide
	Winter Internship	Global Cyber Challenge	(02) Paid Advanced Cyber Security Workshop	(03) Technical Research Paper for Cyber Peace Journal	Open Source Implementation	

Y3 : Innovate

ER-01	ER-02	ER-03	ER-04	ER-05	ER-06	ER-07
Setting up Research Lab	Summer Internship	Cyber Security Research	(01) Free Research Workshop	(03) Technical Research Papers for Cyber Peace Journal	BoF for standards	Engaging in Cyber Peace Corps Activities
	Winter Internship	Global Cyber Challenge	(02) Paid Research Workshop		Submitting Draft in IETF	



Who can join?

Engineering College having Information Technology, Electronics or Computer Science departments and are offering B.Tech/BE/BCA/MCA courses for students.

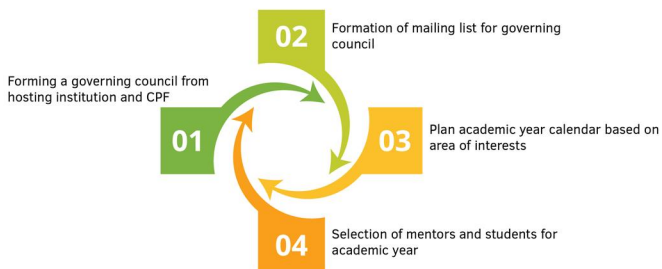
Science colleges having computer science subjects at Undergraduate or Post Graduate Level.

Universities having affiliated colleges offering above mentioned subjects

The process flow to start : Stage 1



The Cyber Peace academic calendar : Stage 2



Year in action : Stage 3



Sample yearly calendar

	Month 1	Month 2	Month 3	Month 4
Cyber Peace Yearly Calendar	<ul style="list-style-type: none"> Cyber Peace Research Lab preparation, MoU Signing 3 Days Introduction Workshop Inauguration of Cyber Peace Research Lab 	<ul style="list-style-type: none"> 5 days Faculty Development Program Identification of Research areas and building team for research activities 1 day Indian IETF Capacity Building program 	<ul style="list-style-type: none"> 3 Day beginners workshop on Cyber Security, Internet Governance and Blockchain (Paid) 	<ul style="list-style-type: none"> Review of activities
	<ul style="list-style-type: none"> 3 days Level 1 Workshop on Cyber Security (Paid) 1 Technical Blog 	<ul style="list-style-type: none"> Summer Internship 1 Technical Blog 	<ul style="list-style-type: none"> Summer Internship 1 Technical Blog 	<ul style="list-style-type: none"> Review of activities 1 Technical Blog
	<ul style="list-style-type: none"> 3 days level 2 deep-dive hands-on workshop on Cyber Security (Paid) Hackathon 1 Articles in Cyber Peace Journal 	<ul style="list-style-type: none"> Winter Internship Hackathon 1 Articles in Cyber Peace Journal 	<ul style="list-style-type: none"> 3 days level 2 deep-dive hands-on workshop on Cyber Security - Hyperledger (Paid) Hackathon 1 Articles in Cyber Peace Journal 	<ul style="list-style-type: none"> Review of activities 1 articles in Cyber Peace Journal



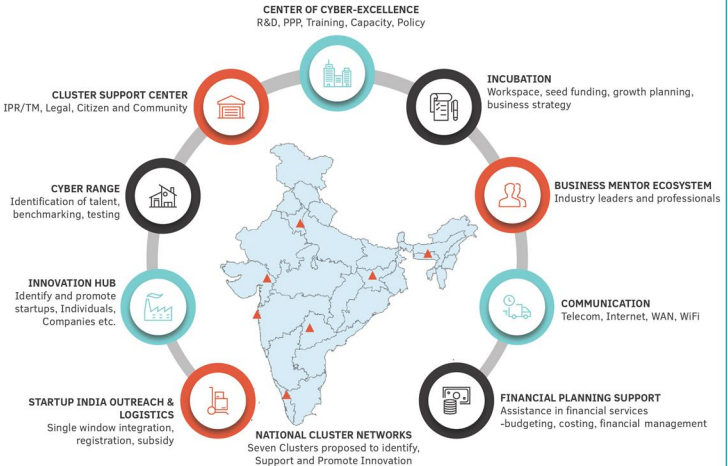
Government establishments will be connected with the academic institution and will identify (a) the skill or specialty of the institution; (b) the relevant challenge / issue faced by the establishment and the manner in which it will be shared.

Once these building blocks are identified, the lead faculty and government representative(s) can plan the required resources, identify the students who will work on the project, timelines etc. Long drawn research projects may have students who work and pass out.

The exposure will also provide visibility of the intelligence and skill of the student while on the project, and the government establishment may consider hiring him/her as he / she passes out of the institute.

The IP from such projects may be patented and licensed for commercial use by the institute. Or, may be carried by the student(s) to build their own startup enterprises.

Overall, such a program will help meet the goals / objectives of Make in India, Startup India and Digital India in addition to the Government's push for Public Private Partnership.

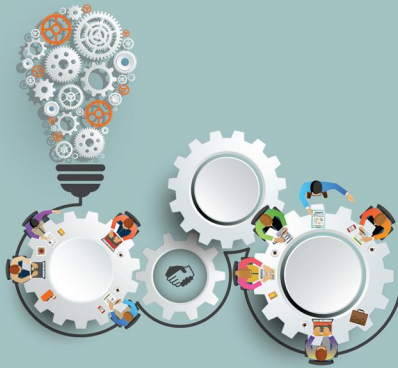


Conclusion

The youth of the country are our promise for the continued prosperity of the motherland, and must be made future-ready at an early age. Close working of the Government with Academia has always produced great results. And, with the participation of the young generation in this partnership it is a recipe for success and for a proactive development bank for national security. Today, the institutions need to be upskilled as much as the nation needs cyber security capability and capacity. We believe that this proposal will bring success in its own small way and contribute to the larger national effort.



MOU & Collaborations



MOU SIGNING WITH KAZIRANGA UNIVERSITY



MOU SIGNING WITH NCIIPC, GOVT OF INDIA



MOU SIGNING WITH GUJARAT TECHNOLOGICAL UNIVERSITY





GLOBAL CYBER CHALLENGE 2017



GLOBAL CYBER CHALLENGE 2017



WORKSHOP AT BIT, MEERUT



INTERNSHIP PROGRAM AT BIT, MEERUT



WORKSHOP AT JHARKHAND RAI UNIVERSITY



WORKSHOP AT ICFAI UNIVERSITY, RANCHI



ROUNDTABLE ON DATA PROTECTION BILL, PEC CHANDIGARH

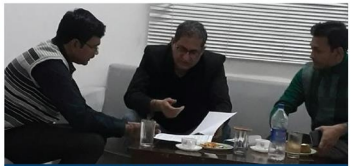




MOU SIGNING WITH INDIRA GANDHI DELHI TECHNICAL UNIVERSITY FOR WOMEN



MOU SIGNING WITH NIT MANIPUR



MOU SIGNING WITH UEM, JAIPUR



MOU SIGNING WITH BIT, MEERUT



MOU SIGNING WITH VJTI, MUMBAI



MOU SIGNING WITH ANSAL UNIVERSITY





ROUND TABLE ON POWER SECTOR CYBER SECURITY AT VJTI, MUMBAI



EXPERT VISIT AT VJTI CYBER PEACE CENTER OF EXCELLENCE



EXPERT VISIT AT VJTI CYBER PEACE CENTER OF EXCELLENCE



CYBER PEACE COE - VJTI WINNER OF CALL FOR PROJECTS AWARD AT GLOBAL CONFERENCE CONGRESS 'CONSENSUS 2018



Draft Annual Calendar 2019 Cyber Peace - Center of Excellence

CoE Engagements

SL	Description	Duration	Type of Event	Intake
1	E-Kawach Project – Internship	All Year	6*	10
2	Cyber Peace Corps Project – Internship	All Year	6*	10
3	Internet Routing and DNS Project - Internship	All Year	6*	10
4	Participation in Cyber Peace Conferences, activities and initiatives	All Year	6*	Fellowship – based on selection
5	Writing for Cyber Peace – Blogs, Journal Articles, Research Papers, Social Media content	All Year	6*	Selection and Review

Community Engagements from Center of Excellence (In the region)

SL	Description	Duration	Type of Event
1	Online safety awareness for Women	All Year	5*
2	Online safety awareness for Senior Citizens and kids	All Year	5*
3	Helping Law enforcement and other agencies in cybercrime issues	All Year	5*
4	Organizing street plays to promote safer online uses in the masses	All Year	6*



Campus Events and Activities

SL	Description	Month	Type of Event (Suggestive)	Days	Participants
1	Hands On Workshop on Cyber Security and Malware analytics		4*	3	30
2	Hands on workshop on Blockchain		4*	3	30
3	Hands on workshop on IoT, Cloud Infrastructure		4*	3	30
4	Seminar on Internet Governance		1*	1	100
5	Faculty Development program on cyber security		3*	5	30
6	Hackathon for talent hunt		5*	2	60
7	Annual Cyber Security Conference (Once in every 4 years)		5*	3	300
8	Summer Internship		5	30	30
9	Winter Internship		5	30	30

*Type of Events

1. Expert logistics reimbursement
2. Expert logistics reimbursement and Honorarium
3. Paid by Institutions
4. Paid by students
5. Co-sponsored
6. Sponsored by Cyber Peace Foundation



State's model for cyber security now a topic of research

Gautam Mazumdar
@thehacknewsindia

RANCHI: Jharkhand's idea of a cyber security model has become a topic of research at Gujarat Technical University (GTU). With an aim to curb rising menace of cybercrimes, GTU in January launched e-Raksha Research Centre that will encourage research and enhance capability to provide solution for issues related to cyber security.

The GTU has asked for Jharkhand's expertise and offered a fee of ₹60 crore to help set up the proposed e-raksha Kanch that is a part of Make in India campaign. Board member of Cyber Peace Foundation GTU and Jharkhand additional director general of police SN Pradhan said the eastern state had copied the idea of cyber security to years back.

"We had been progressing with our e-raksha programme but lack of understanding put the scheme on a back-burner," Pradhan said.

GTU is collaborating with cyber peace foundation to establish a peaceful and harmonious cyber space.

Manufacturing of routers, switches, firewalls, UTM (unified threat management) and other network appliances has been planned under the e-raksha programme.

E-RAKSHA

■ The centre will support 'Make in India' concept by manufacturing routers, switches, firewalls, UTM (Unified Threat Management) and other network appliances

■ It will support the government in protecting critical infrastructure and mission critical services

tions for issues related with cyber security. The research will also support capacity building of the faculties, students and government officers.

Pradhan is hoping Jharkhand will become and the state will adopt soon. Back-up infrastructure was required for the programme but we are now setting up the central room which he said adding that it is already ahead of time in Jharkhand that time.

Pradhan said Jharkhand one of the best data of the police headquarter informed that the government's web portal handle government app run on it.

"It will be helpful as cyber security and open source barriers globally

All for cyber security

ANSRP, MUKESH

Ranchi, Dec. 31: One of the oldest engineering colleges in Asia will receive Ranchi's help to set up a first of its kind community cyber range, which is a virtual environment that is used for cyber warfare training and cyber technology development.

City-based Cyber Peace Foundation (CPF) had signed a memorandum of understanding (MoU) with Maharashtra's Yerramala Jijaji Technological Institute (VJTI) at an event in Mumbai on Thursday night for a period of five years during which it will provide technical inputs and assistances to establish specialised laboratories and systems to enable real-time training exercises.

This new facility will also help various state governments with intelligence input to thwart cyber attacks.

Vinod Kumar founder of CPF who was earlier associated with Jharkhand police as chief technical officer and



Cyber expert Vinod Kumar (extreme left) with officials of VJTI in Mumbai on Thursday. Telegraph picture

helped establish the state's cyber cell, said that the key areas of this multi-dimensional collaboration would also include imparting training in ethical hacking and conducting cyber challenges.

The MoU also envisages conducting real-time cyber war games to identify talented individuals and to generate interest among students and community to build up an army of experts and ethical hackers who in turn will assist

the more important today than ever before and in days to come the need for a strong cyber security system will decide the future of country.

To prove his point, Kumar gave the examples of Legion, an unknown group of people, who had recently hacked Twitter accounts of prominent personalities like Rahul Gandhi, Vijay Mallya, Kavish Kumar and Barkha Dutt.

Kumar further said that financial frauds were the biggest threat to a bank at a time when cashless campaign is underway. "Recently, 12 lakh debit cards of various banks were compromised. Malicious software allowed hackers to extract money off user accounts," he added.

The CPF founder said that it was high time everyone should turn towards cyber safety. "Today, the world is aware of Jammu district in the state more than M.S. Dhoni and Dweepika Patarkota because most of the financial cyber crimes are emerging from there. So, we should pull up our socks," he added.

सायबर सिक्युरिटीनी ट्रेनिंग अपाशे देशमां सायबर क्राइम रोकवा GTUअे ई-रक्षा सेन्टर भोज्युं

को म्यूटर टेकोलोजी अने ई-ट्रनेनेटा जसोपा प्रमाखमां उचयोचना करखे आखे निरुधना करे पत्र प्रखामां भेलांने अपा विषयनी माहित भेवानी सक्रय करे ई-ट्रनेनेटा वपना जना वपराशना करखे लोकोनी सुमाकरीमां वपानी थवानी साथे थली सायबर सभस्यको पर उनी वरु छे. पास रीने सायबर सिस्कोरिटीना प्रको आखे वरे देखा माटे सायबर क्राइमने निवारण माटे गुजरात टेकोलोजीकव युनिवर्सिटी द्वारा गुजरातमां सौ प्रथमवार ई-रक्षा सेन्टर भोजवामां आयुं छे जेमां सायबर क्राइम अने सायबर प्रोब्लेमनुं सोल्युशन सोवपामां आवरो.

सायबर जोर सामे सायबर निविटी खाने सायबर वेन सायबर सिस्मिटी ई पर जोखव वाकरोसामां अेसम्प्रे वदर सायबरने वजना भविष्यनी अग्रयाओ पः

भोजवानी विषयो जेमां वरु पछीना सिस्मिटीसवरे तो अ थी होवामानुं कामः अथवां तेने निवा पसे सायबर निव वेपन खोजा जरुरं पथुं सोवपानी कर खोजा पर वार मुकुं



ई-रक्षा सेन्टर कवा क्षेत्रमां काम करखे

- सायबर क्राइमने रोववानी बेदरे टेकोलोजी सोवपी
- सायबर क्राइमने निवारण वंकर अने सायबर अेसम्प्रेवनी मदद बेवी
- गर्भपेट ओकिर, प्राविट सेक्टर, सुडकर वपरेने ट्रेनिंग आपनी
- सायबर क्राइमना अतरा केस सोव वरवा
- सायबर क्राइमनुं भविष्यनुं वपान वरवुं

ई-रक्षा सेन्टरमां सायबर क्राइम रोकवै सायबर प्रोब्लेमने सामस्याओनुं संशोधन करव



SN Pradhan, ADG, Jharkhand police, J.C. Jaiswal, register, GTU and Dr Akshai Agrawal, VC, GTU at the signing of MoU for e-Raksha

GTU to help students fight cyber crimes

Gujarat Technological University will provide training for its final year students of computers and information technology. The change was incorporated with GTU planning to establish e-Raksha research centre to fight against cyber-crimes. SN Pradhan, additional director general of Jharkhand police said, "In the next 10 years, it will be difficult to commit a crime without leaving a digital footprint. Thus it is necessary for the current generation to learn how to trace it. As of now, there is no ecosystem which can help trace a cyber criminal easily. Exposure and training will be a must for each person."

THE TRAINING WILL INCLUDE RESEARCH ON LATEST TECHNIQUES ADOPTED BY CYBER CRIMINALS

uses from research on latest techniques adopted for cyber crime to capacity building of faculties, students and government officers will be undertaken. The centre will also support "Make in India" campaign by manufacturing Indian routers, switches, firewalls, UTM and other network appliances.

"We will have an international conference each year where knowledge sharing will take place. We will identify problems and give solutions to let students know about it," said J S Jaiswal, registrar of GTU.

Indian Govt Develops Cyber Tivra App For Kids, Against Dangerous Blue Whale & Momo Challenge



Cyber Security Game for Kids - Developed at Royal College University - Gujarat Govt team, Launched by NCPDR, Government of India



WannaCry hasn't hurt India's government, but there have been dangerous, unreported attacks before

Outside of the government, Cyber Peace Foundation, a Delhi-based cyber security non-profit, has uncovered in a project called Honey Net in recent cyber attacks. Under that project, the NGO has set up deliberately vulnerable computer networks in 10 states, including Jharkhand, Odisha, Andhra Pradesh and Karnataka, to invite cyber attacks in order to analyze their nature. They recorded an unusual trend a day before the global cyber attack of May 12.

"The system which usually endures 1-47 cyber attack attempts per day on an average actually endured around 5000 attacks on Thursday" said the founder of the NGO Vikram Bhatia. They have received requests to deal with 13 Ministry defences. These defences include private enterprises, academics, institutes and government agencies, Bhatia said, but did not disclose their identities.

GTUની DRDO સાથે મળીને ઈ-રક્ષા કેન્દ્ર સ્થાપવા દરખાસ્ત

» ખંડણીની નવી મોડલ ઓપરેટીંગ 'રેલ્સમોવે' નો ક્રિકેટ શોધખાતી ડવાઇઝ

નવરાટ્રીના સમયે રાજ્યમાં ૧૦-૬-૧૬ ડાઉનલોડ ૨૬ નો લોકોએ પાનિ વર્કિંગ



GTU launches centre to fight cybercrime

Press Trust of India | Ahmedabad
Last Updated on January 28, 2015 10:15 IST



DRDO ટીમ અને જીટીયુ એક્સપર્ટ કહ્યું કે, 60% મોબાઇલ અપ્સ આપણા માટે જોખમી



DRDO & GTU to set up Cyber Security Centre

PTI Updated On 26, 01, 2015 07:00 AM



જીટીયુની મુલાકાત કોન્ફરન્સ રિસર્ચ એન્ડ ઓર્ગેનાઇઝીંગ ટીમ લીધી હતી. ભવિષ્યના સાયબર ગુનાઓનું મૂળ અર્થઘટન સહીત તથા આ બાબતોને ધ્યાનમાં લઈ જી સાયબર ક્રાઇમના નિવારણ માટે ઈ-રક્ષા કેન્દ્ર સ્થાપાઈ રહી રહ્યાં છે. @ahm.cb

DRDO Research and Development Organisation (DRDO) in association with Gujarat Technological University (GTU) today decided to set up a Cyber Security Centre (called as e-Raksha Research Centre).

The announcement was made by Dr. N. K. Kumar, distinguished scientist and chief controller of research and development, DRDO, Mumbai in a release issued by GTU.

સાયબર પીસ ફાઉન્ડેશનના પ્રમુખ વિનિત કુમારે કહ્યું કે 'રેલ્સમોવે' કે મારવેલ જેવા હુમલાઓ એટલી વાઈરસ વિસ્ફોટ પારખી શકતી નથી. આવી પરિસ્થિતિમાં માત્ર અગમચેતી જ ઉપયોગી બને છે. નક્કલવાદ પ્રબલિત એરિયામાં હવે નક્કલાર્થિસ પણ કેરોનોલોજીનો



અને વિચાર્ચિનો લેવામાં આવશે.' જીટીયુના ચાન્સેલર અશ્વ પત્રવાલે સાયબર ક્રાઇમ વિશે માહિતી આપતા કહ્યું કે, 'આજનો યુવાન સ્પાઈકોનેમી તેને મનુગમતી એક્સિટેશન ડાઉનલોડ કરે છે, પણ વણા લોકોને પછર નહીં લોખ કે આમાંની 60 ટકા એક્સિટેશન આપણા માટે જોખમકારી છે. સાયબર ક્રાઈમી ક્રેનારા વ્યક્તિઓ આ કારણે

Cyber security labs to be set up by next yr

Somdutta Chatterjee
Ranchi: Cyber forensics, intrusion and incident laboratories will be set up in the state capital to tackle incidents of rising cyber crimes by January next year. The initiative to set up these research hubs centres is being undertaken by Delhi Public School, Greater Ranchi (second school of DPS group here) in collaboration with Cyber Peace Foundation.
The state infrastructure will be made at Ranchi in the next one year. As of now, schools/diploma centres setting up laboratories near Birla Institute of Technology, Mesra, with the help of Delhi Public School, Greater Ranchi by August '15, said Cyber expert, Vinay Kumar, associated with Cyber Peace Foundation, adding the concept is a pilot project and will be expanded later. According to Kumar, school parents, entrepreneurs and government author-



The cyber meet at a city hotel on Tuesday

chief executive officer Dr. Nageshwar Ramprasad.
Meanwhile, former chairman of DPS Greater Ranchi and Advisor of Cyber Peace Foundation, Kishor Kishore, said a software will be developed to predict and observe before an attack on children.
Added upon the need of such laboratories, Kumar said Jantar is now known as cyber crime hub across the nation, indicating a need for a rehabilitation programme to keep a check on such incidents.

Vivek Jagpal and Pyramil Cyber Security are collaborating for the Cyber Peace Foundation White, Science and Technology Centre for Innovation Laboratory, Anandkand Open Cell Cyber Club is working for the Innovation Laboratory. A cyber crime legislator will be set after the launch of the laboratory, Vinay Kumar said.

With an aim to curb rising menace of cybercrimes, Gujarat Technological University (GTU) here has launched e-Raksha Research Centre that will encourage research and enhance capability to provide solution for issues related to cyber security

"GTU has launched e-Raksha Research Centre where various activities from research on latest techniques of cybercrime to capacity building of the faculties, students and government officers will be undertaken," a statement from GTU said here yesterday.

PRSD RELEASES

Cyber Security will be the biggest challenge for Smart Cities & IOT

Posted by GTU on MAY 9, 2016

Ahmedabad: Cyber Security will be the biggest challenge for upcoming Smart Cities and Internet of Things (IoT). Android attacks will be major problem, as number of Android apps is increasing. There will be more vulnerability to secure database. To contribute for the social cause, Gujarat Technological University (GTU) is strengthening research in cyber security. Dr. Akhail Aggarwal, Vice Chancellor of GTU said,

A team of Defence Research and Development Organization (DRDO) including Dr. G. Athithan DS & CCR&D (SAM), DRDO, Dr. Arvind Bhatia, OSD, CCR&D (TM), DRDO visited GTU for exploring the proposal to set up e-Raksha Centre for joint research in cyber security. Dr. Aggarwal said that the IoT is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and





e-raksha
making netizens responsible & safe
RESEARCH CENTRE



CYBER PEACE FOUNDATION



INDIA : +91 82350 58865



USA : +1 71624 11555



UK : +44 20 32870765

www.cyberpeace.org

secretariat@cyberpeace.net



[/cyberpeacefoundation](https://www.facebook.com/cyberpeacefoundation)



[/cyberpeacengo](https://twitter.com/cyberpeacengo)



[/cyberpeacefoundation](https://www.youtube.com/cyberpeacefoundation)