CYBER DEFENCE

CONCEPT BY

DOCTOR
TANMAY S DIKSHIT

FORWARD BY

BRIGADIER (RETD)
HEMANT MAHAJAN

EFFECTS OF CYBER SECURITY ON THE DEFENCE & NATIONAL SECURITY

AUTHOR - SHIVKUMAR BALRAJ NILI

Index

AUTHOR'S INTRODUCTION

DR. TANMAY S DIKSHIT

- The book concept was idealised by Tanmay S Dikshit
- He was awarded 2 State Awards (Government of Maharashtra) and 1 President Award (Government of India)
- Called on Renowned TV News & Radio Channels for Interviews & Bites, aslo published 250 + articles in print & web media
- Prestigious Hall of Fame recognition as an Information Security Researcher awarded for contribution for reporting security issues in their system (U.S. Department of Defense, AT&T, Mastercard, Flipkart)
- Dr. Tanmay S Dikshit is a Visiting Faculty at Department of Information Technology, Sanjivani College of Engineering (An Autonomous Institute), Kopargaon
- Published International 6 Amazon ebook and 6 Udemy E - Courses
- Invited as Board of Studies Members from Shivaji University (Kolhapur)Savitribai Phule Pune University (Pune) and Sandip University (Nashik)
- Highly Energetic Speaker of Digital Devices's Security and Graphology Science.
- Certified Trainer for Cyber Security Investigation & Digital Forensic Analysis, Brain Computer Interface, Artificial Intelligence, Machine Learning and competent to conduct seminars and Hands on Workshops
- Has delivered these workshops and Seminars for Diploma and Degree students as well as teaching staff for Government and Private Engineering and Other's colleges
- Has facilitated tie-ups & MoUs with many Engineering colleges for conducting Guest Lectures & Hands on Training / Webinar / STTP / FDP on the similar subject
- He is rhetorician and well versed trainer and accords training to Military personals, detectives and all the security forces in which cyber security is required
- Invited as spokesperson at reputed organizations, companies and educational Institutions / Universities to shed light on the major aspects of Cyber Domain
- Organizes events, workshops & Awareness Campaigns regarding the same
- He has 25+ years of Experience in Technology and has completed 50+ International Professional Level Certifications
- Please visit https://www.tanmay.pro and WhatsApp 8149256703

SHIVKUMAR NILI

CYBER SECURITY ANALYST

PROFESSIONAL SUMMARY

I am a skilled Cybercrime analyst with expertise in Cybercrime & Real-time case studies. I like to preach awareness about Cyber Security.

CORE COMPETENCIES

Cyber crime & Real time Case Studies
Cyber Forensics Analysis
Live Forensics - Acquisition of Random Access Memory
Cryptography
Stenography
Data Storage Techniques
Data Recovery
Ensuring Data Integrity - Hashing

CERTIFICATIONS

Hand on Session on Cyber Forensics - MSME (PPDC)
Cyber Security & Blockchain Technology - (AICTE)
General Online Safety, Password & Wifi Security And Mobile Security - (C-DAC, Noida in association with CERT-In)
Cyber Security, Cyber Forensics and Real time Case Studies - (Cyber Sanskar)
Cyber Crime Analyst - (Udemy)
Cyber Forensics Investigator - (Udemy)
Cyber Psychology Consultant - (Udemy)

PROFESSIONAL HISTORY

CYBER CRIME ANALYST

Cyber Sanskar

- Working as Cyber crime Analyst and Cyber Forensics Investigator under, Mr.Tanmay S Dikshit (CCI, CEH, ECSA, PGDCL, Cyber Forensics Expert)

- I also spread Cyber security Awareness lectures to School & college students.

ACADEMIC BACKGROUND

SAVITRIBAI PHULE PUNE UNIVERSITY

Undergraduate Degree | 2022

BSc in Defence and Strategic Studies (persuing Last year)

MAHARASHTRA STATE BOARD

HSC | 2017, Pune.
SSC | 2015, Pune.

REACH ME AT:

Mobile: 9373334173
Email: shivkumarnili08@gmail.com

INTRODUCTORY REMARKS BY

BRIGADIER HEMANT MAHAJAN, EXPERT ON NATIONAL SECURITY

I compliment Dr Tanmay S Dikshit, Cyber Forenscis Expert & Shri Shivkumar Balraj Nili, Cyber Security Analyst for having produced an excellent book on CYBER DEFENCE, CYBER TECHNOLOGY & NATIONAL SECURITY. It is a book which must be read by everybody connected with the cyber world. It gives Practical Guidance, techniques and tips for securing your cyber environment.

The book broadly covers introduction to Cyber Crimes & Cyber Security in the first chapter. In the next chapter it covers Industrial Revolution 4.0 and impact of cyber crime on National Security. In chapter 3 book covers introduction to Brain Computing Interface Technology and its impact on National Security, Drone Technology and Intelligence and Surveillance. Lastly the book gives you date lines of various Cyber Crimes over the years, which clearly brings out the grave threat posed by Cyber Crimes. Guarding Cyber Borders Equally Important.

As an Army man **I was involved in guarding India's land borders, sea borders and space borders all my life.** How ever since last 15 years, the **Cyber Borders** have become equally important. Cyber borders have to be guarded both at National Level ,at Institutional Level and at Individual Persons Level.

Cyber Security is the practice of protecting systems, networks, and programs from digital attacks. These cyber attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes. It is the protection of internet-connected systems such as hardware, software and data from cyber threats. The practice is used by individuals and enterprises to protect against unauthorized access to data centers and other computerized systems.

Cyber Security Needed By All Cyber security can broadly be categorized into Critical Infrastructure Security, Application security, Network Security, Cloud Security, Internet of Things security and many more fields.

Although it is necessary for all to instill a sense of Cyber Security, many Institutions like Healthcare, Small Businesses, Government Agencies, Manufacturing, Financial Institutions, Education and energy, Defence Services, Central Armed Police Forces, Police require it.

Learning About Cyber Security ?

As you build the skills you'll need a introductory course, Learn a little every day, practice in simulated environments and mix it up with workplace skills. Dr Tanmay Dikshit's book will greatly help you in this endeavor. Examples of Network Security includes Antivirus & Antispyware Programs, Firewall that block unauthorized access to a network & VPNs (Virtual Private Networks) used for secure remote access.

Generally, the disadvantages of Cyber Security are, Firewalls are tricky to be set up . Firewalls that are incorrectly constructed may block users from engaging in certain Internet activity till the firewall is configured correctly. It slows down the system.

Cyber Attacks A Threat For All can cause electrical blackouts, failure of Military equipment, and breaches of national security secrets. They can result in the theft of Valuable, Sensitive Data. They can disrupt phone and computer networks or Paralyze Systems, making data unavailable.

Cyber security can be learnt in few weeks. The time it takes to know cyber security depends on the individual learning it. You could join Dr Tanmay Dikshit's classes for faster learning. The job of defending against increasingly advanced threats on a daily and hourly basis is increasing day by day. The field is highly dynamic; every day presents a different scenario with new riddles to solve. Furthermore, Cyber Criminals are constantly developing innovative ways to break into systems and hack people.

It is very clear that Cyber Security is no more a subject of experts or professionals but it is a subject which is **Very Important to a common Indian working in any field, at all times .**

In the Russia Ukraine war , **Cyber War** is being fought extensively. But this was not due entirely to the preparation and Cyber Assets of the Ukrainian Government. Much of the credit here goes to the Private Sector. Without the fast work of Private Sector Actors such as Microsoft, which rapidly mobilized to counter a meticulous ransomware campaign, Lumen Technologies, which literally cut .ru domains from the internet, and SpaceX, which deployed Starlink internet service to Ukraine, the effect of Russian Cyber Attacks could have been destabilizing and granted Moscow the tactical advantage and confusion it so desired.

Cyber Security not just as a National Security, but International Security Challenge.

Therefore this book concepted by **Dr Tanmay S Dikshit** will be very useful to everybody interested in keeping his cyber boundaries secure. I am sure that the book will be received very well by the environment and second reprint will be published very soon.

I wish **Dr Tanmay S Dikshit** and **Shri Shivkumar Balraj Nili** all the success in his future endeavors.

Brigadier Hemant Mahajan, YSM

Pune, 29 Aug 22

WHAT IS CYBER ?

INTRODUCTION TO CYBER

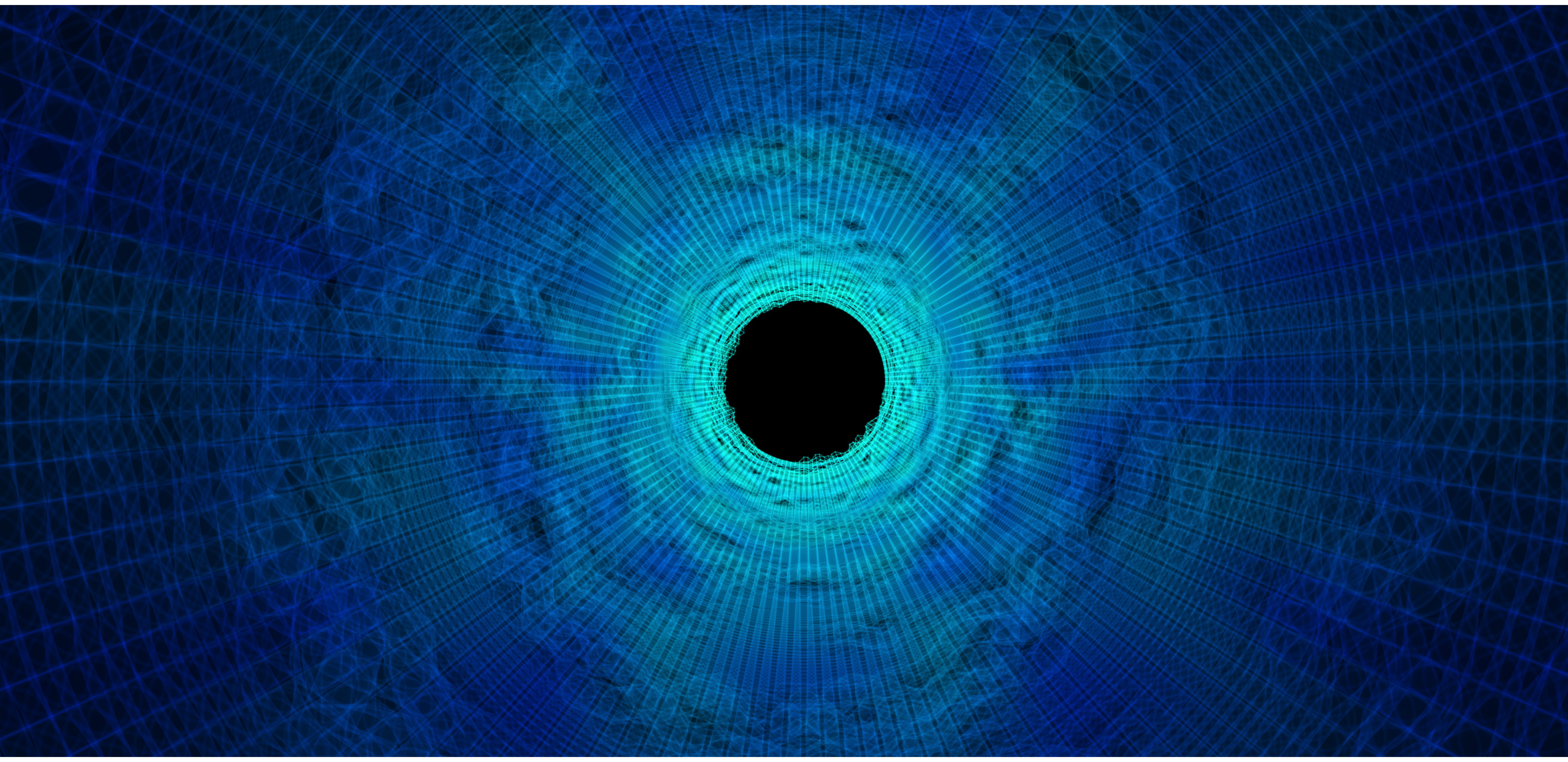
WHAT YOU SHOULD BE AWARE OF

Cyber is a Greek word, which is use for person, or idea as part of the computer and information age, that is taken from cybernetic, which is related to the idea of governing.

The meaning of the word Cyber is, all those devices which can be connected to internet is called cyber, e.g.: computer, mobile, tablet, laptops, and etc, this are some devices which falls under the cyber category.

Origin of Cyber : There was a man named Norbert Wiener who was a mathematician, he wrote a book named Cybernetics in the year 1940, and he was the one who originated the term cyber in he's book Cybernetics. There are some much same word in which cyber is interconnected and those words are identified as, **Cyber Space, Cyber Security, Cyber Crime, Cyber Attack, Cyber Bullying & Cyber Forensics.**

CYBER SPACE



Cyber Space : The term cyberspace coined in 1982 by the American-Canadian author William Gibson. In one of he's stories published in Omni magazine and then in his book named Neuromancer, that was a science-fiction novel in which, Gibson described cyberspace as the establishment of a computer network in a world fill up with artificially intelligent Neuromancer beings. Cyberspace is a figure of speech for describing the non-physical topography created by computer systems.

CYBER SECURITY

Cyber Security : Cyber Security is to keep secure, the cyber devices and processes the design to protect computers, networks, data and all the cyber devices from illegal access, vulnerabilities, and the attacks perform through internet by cybercriminals.

CYBER ATTACK

THE WORLD NEWS

$1.00

Since 1883

YOUR NUMBER ONE SOURCE FOR HEADLINES

CYBER ATTACK!

24,000 FILES STOLEN IN LATEST ATTACK

are now

IMPACT OF ATTACKS REACHING INTO THE ECONOMY

are being made by local industry

DEFENSE DEPARTMENT TO BEEF UP VIRUS PROTECTION

For updated information please visit our afternoon edition

Water consumption up the country. Efforts local

Cyber Attack : The unauthorized or illegal access on Photos, Videos, Audio, Documents and on any private files which carries confidential information through computer system or by any cyber devices is called Cyber Attack.

CYBER BULLYING

Cyber Bullying : The term Cyber Bullying is coined by Canadian educator Bill Belsey, and there are some other terms for cyber bullying are, e-bullying, SMS bullying, mobile bullying, online bullying, and digital bullying, or Internet bullying" any form of online harassment is called Cyber bullying.

CYBER FORENSICS

Cyber Forensics : There are some Cyber Forensics Tools which are used to gather digital evidence, means any type of wrong or illegal activity which takes place through cyber devices by anyone then the cyber forensics tools are used together digital evidence to provide a conclusive description of cyber crime activities and catch the criminals is called Cyber forensics.

INTRODUCTION TO CYBER CRIMES

We live in a Cyber World, where there is an abundance of information which is freely flowing and easily available to access. Computers, Mobile, Digital Cameras and other electronic or Cyber Gadgets have become an indivisible part of our daily lives. On the other hand, confidentially, lack of defined boundaries and restrictions of information access, and a growing dependency on technology has attracted criminals to use these as a medium of conducting criminal activities. Such acts are known as cybercrimes. When a cybercrime is reported, it gets investigated and some suitable law may form to check similar cybercrimes in future.

A Cyber Crime can be defined as any unlawful or illegal activity which can be responsible of using cyberspace as a tool or target. The word cyberspace encompasses electronic devices with the capacity of storing or processing data (electronically).
Cybercrimes are committed in cyber space, but are not limited to crimes committed using the internet or any cyber devices. Any digital devices or medium may be used in this sense, mobile phone, CD's, DVD's, microwave ovens or even GPS navigation system would all be considered cyber space.

Types of Cyber Crimes : There are around 22 types of Cyber crimes which are known till the date as given below, Cyber Defamation, Cyber Pornography, Cyber Bullying & Stalking, Cyber Terrorism & Cyber Warfare, Data Alteration or Diddling, Denial of Service Attack (DoS), Email Bombing, Email Spoofing, Digital Forgery, Intellectual Property Theft, Internet Time & Bandwidth Theft, Online Gambling, Phishing Attack, Salami Attack, Sale of Illegal Articles, Source Code Theft, Voyeurism, War Driving, Identity Theft, Web Jacking, Web Defacement, and Malware Attacks.

This are the count of 22 types of cyber attacks till now, This all are created by various hackers in this several years, whatever cyber crimes are performed in all over the world till this day, are done by these types of attacks only, and also there are so many cyber attacks which are been performed in real time and also done, through this types of attacks only. Leaving this 22 types of attacks, we have heard about many more others names but all those attacks fall under phishing or malware categories. (e.g. email phishing, https phishing, virus, worms, trojan horse, ransomware and spyware)

INTRODUCTION TO CYBER SECURITY

Cyber Security or Information Security (IT security) is the protection of computer Systems & Networks or all those devices that are connected to the Internet which is also called Cyber, against disclosure of information, theft or damage to hardware, software or cyber data, as well as against disruption or diversion of services provided.

The first cybersecurity was created in the year 1970 by BBN Engineer Technologist Bob Thomas, who wrote code for a program that could move between computers connected via the ARPANET (the technical foundation of the Internet). His program had no malicious intentions but cheekily displayed the message "I'm a creeper: catch me if you can!" So basically, cyber security is a technology that handles the design to protect computers, networks and data from unauthorized access. vulnerabilities and attacks by cybercriminals via the Internet.

This area has grown exponentially due to increased reliance on computer systems, the Internet, and wireless networking standards such as Bluetooth and Wi-Fi, and the growth of "smart" devices, including smartphones, tablets, laptops, desktop computers, televisions, and various other Internet-enabled (cyber) devices objects (IoT). Cybersecurity is also one of the most important challenges in today's world, due to its entanglement, both in terms of political and technological uses. Its main objective is to ensure system reliability, data integrity and privacy.

The term cybersecurity applies for business to mobile computing, and is divided into several common categories such as network security, application security, information security.

Network Security : A process of protecting a computer network from attackers, whether it might be a targeted attackers or malware.

Application Security : Main target is to keep software and devices threat-free. A compromised application can provide access to data intended to protect it. Effective security starts at the design stage, before a system or device is deployed.

Information Security : Protects the integrity and confidentiality of data, both in storage and in transit.

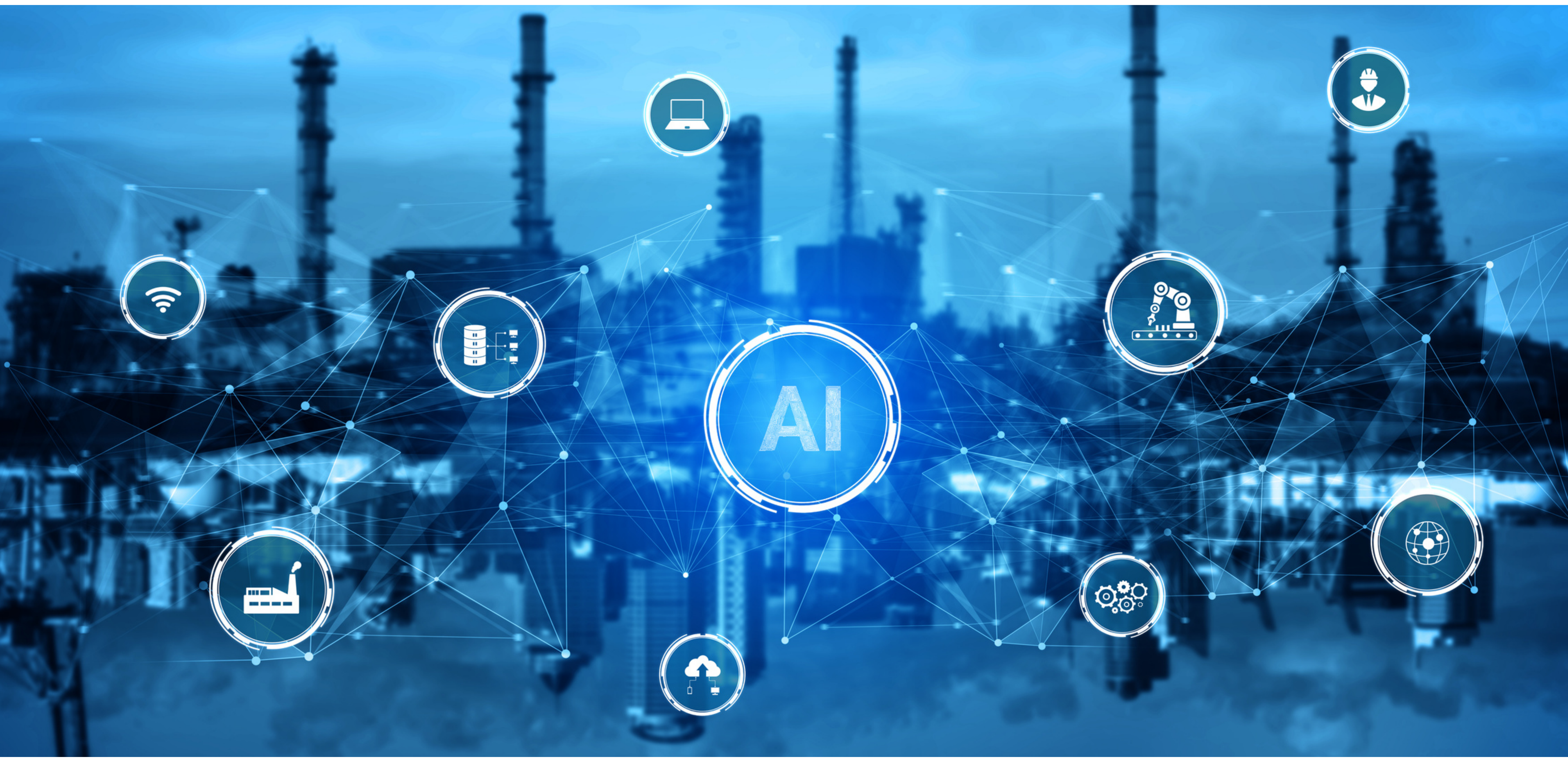
INDUSTRIAL REVOLUTION 4.0

INDUSTRIAL REVOLUTION 4.0

The Fourth technological revolution, Industrial 4.0, thinks of speedy changes in technologies, industries, and social patterns and processes within the 21st century as a result of increased communication and mechanization. The term has been generally utilized in scientific literature, and in 2015 it became fashionable Klaus Schwab, founding father of the World Economic Forum and Executive Chairman. Schwab asserts that the perceived changes aren't only a result of improved efficiency, but also a big shift in industrial capitalism.

Part of this phase of industrial change is the integration of technologies such as AI, gene-splicing, and advanced robots which separates the lines between the physical, digital, and biological worlds.

Throughout this point, some important changes have taken place within the way the global production and supply chain operates continuous production of standard production and industrial processes, using modern technology, high-speed machine communication, and Internet of Things. (IoT). This integration leads to increased automation, improved communication and self-monitoring, and therefore the use of smart devices that can be used to analyse and diagnose problems without the need for human arbitration.



It also represents the social, political, and economic changes from the digital age within the late 1990s and early 2000s to the era of deep-seated communication that separates the use of omni and the common use of technology across society (e.g., metaverse) that changes ways people know and know the planet around them. It sets bent create and penetrate the improved realities of society compared to the natural senses and human industry capabilities only.

Let's see the history of commercial Revolution, how exactly it came in power and the way it evolves till IR4.0, The term "Industry 4.0" was publicly introduced in 2011 at the Hannover Fair. The Hannover is one among the world's largest trade fairs, dedicated to the subject of industry development, which is persisted the Hanover Fairground in Hanover, Germany.

The talk about the Fourth Industrial Revolution was firstly introduced by a group of scientists who developed a high-tech strategy for the German government. Klaus Schwab, executive chairman of the planet Economic Forum (WEF), introduced this statement to a wider audience during a 2015 article published by Foreign Affairs. The "Success of Fourth Industrial Revolution" was the theme of the 2016 Annual Meeting of the planet Economic Forum, in Davos-Klosters, Switzerland.

On October 10, 2016, the Forum announced the opening of its Fourth Industrial Transformation Centre in San Francisco. This was also the title and title of the 2016 Schwab book. Schwab incorporates during this fourth era technologies that integrate hardware, software, and biology (cyber-physical systems), and emphasizes advances in communication. Schwab expects this era to be marked by the development of emerging technologies in fields such as robotics, artificial intelligence, nanotechnology, quantum computing, biotechnology, internet of things, industrial internet, extended compliance, fifth generation wireless technology, printing 3D, also as fully independent vehicles.

TECHNOLOGIES OF INDUSTRIAL REVOLUTION 4.0

The 4th Industrial Revolution is a combination of advances, which includes Cyber-Physical Systems (CPS), 3D Printing, Mobile Technology, Cloud Computing, Internet of Things (IOT), Big Data Analysis, Cyber Security, Artificial Intelligence (Al) & Machine Learning, and Robotics. Introducing four themes summarizing Industrial 4.0: Interconnection, Transparency of information, technical assistance, Fixed decisions.

Interconnection : The ability of machines, devices, sensors, and individuals to connect & communicate with others through the Internet of Things, or the human internet

Transparency of Information : The light provided by Industry 4 technology provides operators with a wide range of information to make decisions. Inter-connectivity allows operators to collect large amounts of data and information at all points in the production process, identifying key areas that can benefit from development to maximize efficiency.

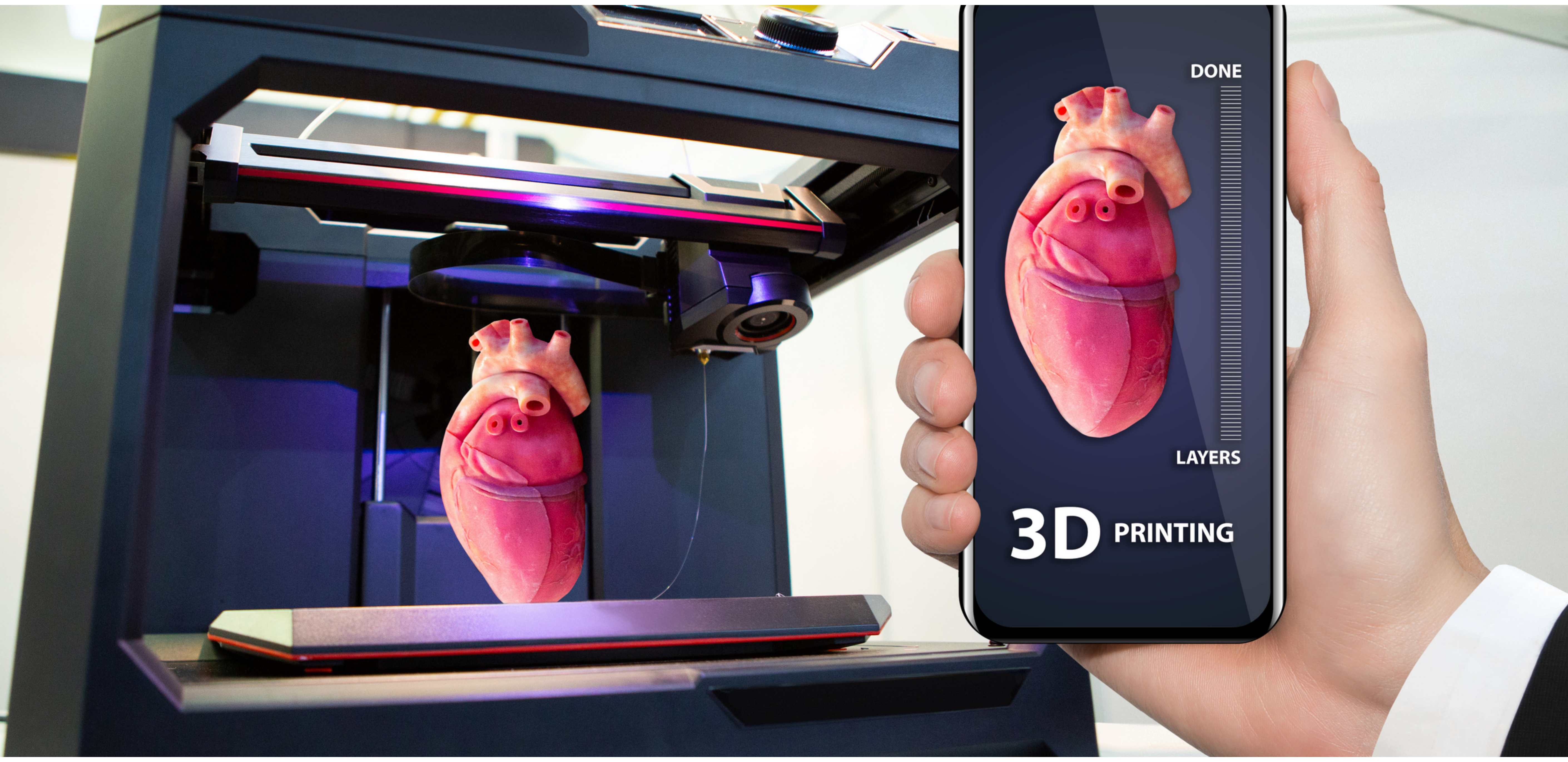
Technical Assistance : The technical centre for decision-making & Problem Solving programs, as well as the ability to assist people with difficult or unsafe tasks.

Fixed Decisions : The ability of cyber physical systems to make decisions on their own and to perform their functions as independently as possible. Only in the event of a difference, disruption, or conflicting intentions, the functions are transferred to a higher level.

The application of the Fourth Industrial Revolution operates through; Mobile devices, Internet of things (IoT) platforms, Location Detection Technologies (electronic identification), Advanced human-machine interfaces, Authentication and fraud detection, Smart sensors, Big analytics and advanced processes, Multilevel customer interaction and customer profiling, Augmented reality / wearables, On-demand availability of computer system resources, Data visualization and triggered "live" training.

Mainly these technologies are categorized into some major components, which defines the term “Industry Revolution 4.0”. The technologies are, 3D Printing, Mobile Technology, Cloud Computing, Internet of Things (IOT), Big Data Analysis, Artificial Intelligence (AI) & Machine Learning, and Robotics, Cyber Physical Systems (CPS), Smart Sensors & Cognitive computing.

3D PRINTER



3D printer constructs three-dimensional object from a digital 3D model. It can be referring to variety of processes in which material is deposited, joined under computer control to create a three-dimensional object, with material being added together (such as mouldable material, fine grains being merge together), in layers. This 3D printer can be use in Defence sector, for rapid production, generally it takes months to produce the necessary tools, Therefore, the defence industry should use 3D printing technology to reduce the time required for product development. It also creates customized parts for specific functions. Instead of carrying parts and pieces for all possible configurations, soldiers can directly use these systems to manufacture parts based on demand. (E.g., the US Army can now 3D print customized drone airframes tailored to a given mission's specific needs). Many parts & components of defence equipment are made using expensive materials such as titanium. Titanium is one of the expensive materials, such materials can be efficiently managed and used in 3D printing without much wastage. 3D printer can help in reducing and managing cost of defence industry.

CLOUD COMPUTING

The cloud enables users to access the same data in almost any device. Cloud servers are located in data centres all over the world, servers that are accessed to the internet, and the software and databases that runs on those servers, the computing & storage takes place on servers in a data centre, that's why we can log in to Instagram, Facebook, Gmail, Google, account from any devices n we can get our full data like files, applications, photos, & videos, as it is. And cloud storage provides like Dropbox and Google Drive. There are almost companies store their data in cloud storage, because once it stores to Clouds storage, the data remains secure. This is how Cloud make it easier for companies to work internationally, because employees and customers can access the same files and applications from any location and at any time.

Some hackers, also try to hack Cloud system to destroy the company’s data or any person’s data, but it's not possible to destroy the data from cloud storage, because Cloud stores their whole data in data centres, and data centres are located in multiple countries, It's the great thing of cloud that it has multiple data centres all over the world. Cloud rotates the whole data from one data centre to another after every certain hour, and data centre keeps the backup of whole data before it shifts to another data centre, it means in every data centre cloud keeps backup of whole data. So, it's not possible to destroy clouds data.

INTERNET OF THINGS

All those devices which connects to internet or WIFI are called Internet of Things, for example, Mobile, Tablet, Laptop, Desktop, AC, washing machine, Television, Smart Watches, Smart Cars, Satellite, Surveillance system, Drones, Laser guided missiles. This all are smart devices which can be use from any were through Mobile, Tablet, Laptop or Desktop.

BIG DATA ANALYSIS

Big Data is a collection of data that is huge in volume, yet growing vastly with time. It is a data with so large size that none of traditional data management tools can store it, People, organizations, and machines now produce massive amounts of data. social media, cloud applications, and machine sensor data are just some examples, but more vast data then this is created by GPS, Tracking.

ARTIFICIAL INTELLIGENCE (AL) & MACHINE LEARNING (ML)

AI is the ability of a computer controlled by a computer to do tasks that is usually done by humans, for example to recognize human gender, face identity with name, voice identity, current temperature status, and recognition of hand writing of person. AI can also use as digital personal assistances and machine translations for example Google's Alexa or I phone’s Siri and AI is also uses in smart cars and smart homes.

Usually Artificial Intelligence (Al) & Machine Learning (ML) technology can be use near airports, companies, societies and in schools & Colleges to recognize correct people by identifying their faces with name and by their gender. This could also help to catch evil minded people, and this technology also identify temperature through which system can identify whether any person is suffering from any diseases and all. Some companies also use robots as receptionists or helper instated of employees, these robots are also type of AI, with multiple qualities.

CYBER PHYSICAL SYSTEMS

A Cyber-Physical System (CPS), or intelligent system, may be a computer system in which a particular system is controlled or monitored by computer algorithms. In cyber-physical systems, physical and software components are deeply interconnected, capable of operating at different spatial and temporal scales, exhibiting many various behaviours, and interacting in changing ways and contexts. CPS covers a good range of methods, including cybernetics theory, mechatronics, design and process science. Process control is usually referred to as embedded systems. In embedded systems, there's often an emphasis on arithmetic and little on the tight coupling between arithmetic and physics. CPS is additionally similar to the Internet of Things (IoT), sharing the identical basic structures; however, CPS produces a better combination of gene interactions and statistics.

Examples : of CPS include the smart Grid, autonomous vehicle systems, medical Monitoring, Industrial Control Systems, Robotic Systems, Autonomous Pilot Avionics. Antecedents of Cyber Physical Systems are often found in a variety of fields such as aerospace, automotive, chemical processes, public infrastructure, energy, healthcare, manufacturing, transportation, entertainment, and consumer electronics.

SMART SENSORS

Sensors and metals drive the central renaming force not only in Industrial 4.0, but also in other "smart" megatrends like smart manufacturing, smart mobility, smart homes, smart cities and smart industries.

Smart sensors are devices that produce data and enable additional functionality from self-monitoring and preparation to state-of-the-art system testing. With the facility of wireless communication, they reduce the quantity of input effort and help detect a dense network of nerves.

The importance of sensors, measurement science and intelligent evaluation of Industry 4.0 are recognized and approved by various experts and have already led to the statement "Industry 4.0: nothing are often done without sensor systems."

However, there are several problems like error synchronization time, data loss, & handling large amounts of collected data, all of which limit the implementation of complete systems. Additionally, other limits to those features are battery power. One example of the mixing of smart sensors into electronic devices is the story of a smart watch, where the sensors receive data from the user's movement, process the info and, as a result, provide the user with information about the number of steps. they went through the day and re-converted the info to calories burned.

IMPACTS OF CYBER CRIME & IR4.0 ON DEFENCE SYSTEM & NATIONAL SECURITY

We are living in 21st century, where we are actually living in Cyber World, where cyber is a part of our daily life, because as we are turning our lives into modern lifestyle, with internet being an indivisible part of it. This is also one of the reasons where cybercrimes are increasing all over the world, till now we have seen many types of war, it might be nuclear, biological, or a war with weapons, but now, in this modern cyber world, it will be totally different kind of war, we going to face, which will be totally based on electronic devices or we can say cyber devices which is called CYBER WAR.

Basically, Cyber war is the war in which mobiles, computers, laptops and tablets are used, in short all cyber devices can be use in cyber war to harm opponents or any particular victim's cyber devices, virtually without knowing anyone and there are many ways through which it can be possible, e.g.; Mobile Technology, Cloud Computing, Internet Of Things (IOT), Big Data Analysis, All this technologies can be used to harm the people, because all this technologies which we use in our daily life is the big reason for cyber war, because it hits bulk of people. This happens because people are using smart devices but most of them don't know how to use it safely and securely, these people can be trapped easily by cyber attackers, and can be defamed or lose their private data, it might be photos, videos, documents or any Confidential Files.

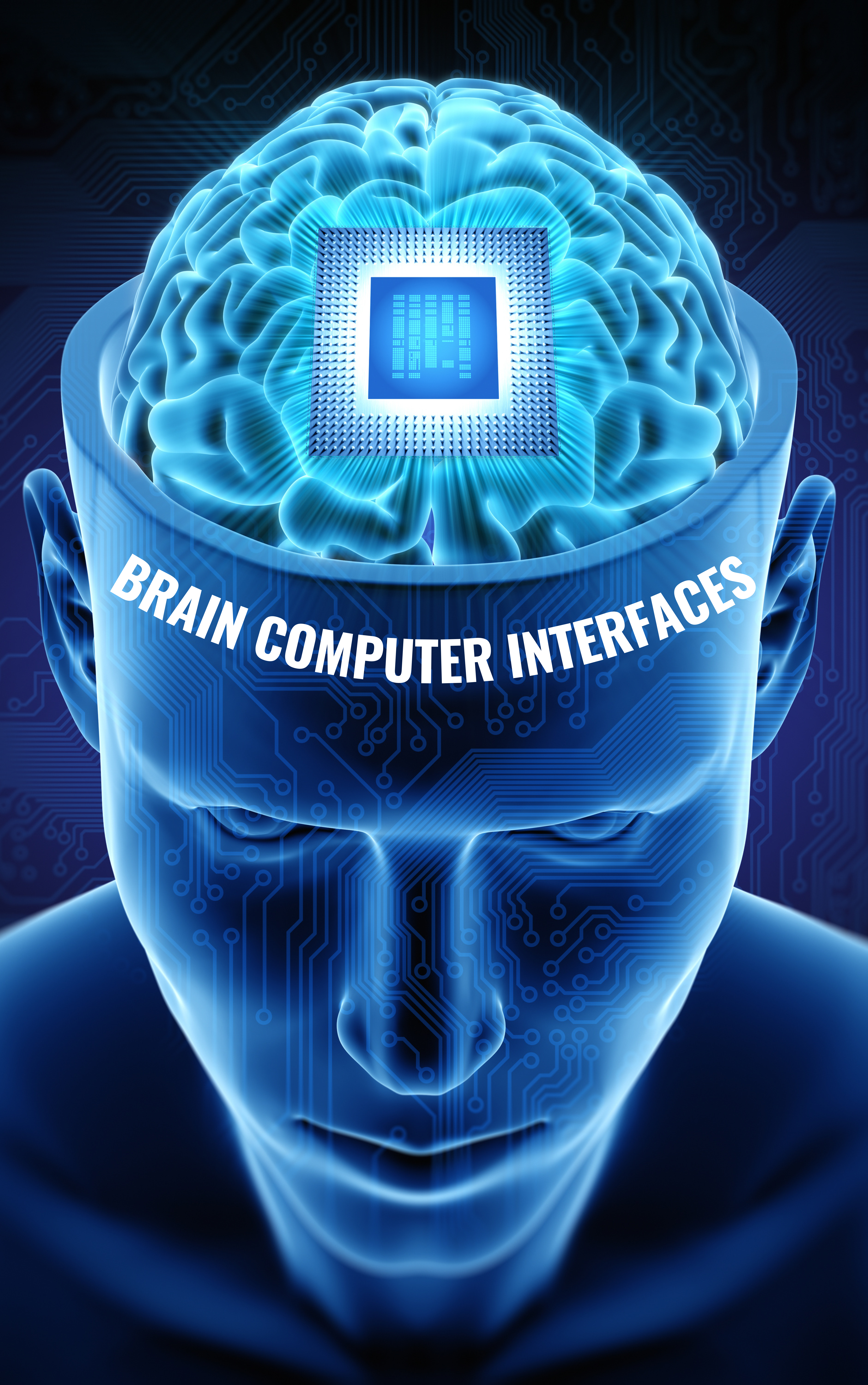
When a single person becomes a victim of cyber hacker, then it can be an issue of that particular person but when thousands of people become a victim by a Cyber Hacker then it becomes a National issue and threat to the National Security.

In a recent event, **Ex. Army chief of India, General M M Narvane** said that, Info security is the biggest challenge to our National Security and in Defence System, in the present situation, which can give a strong shock to the economy and can handicap government machinery also. In his virtual address on the topic of "India's National Security Scenario Past, Present and Future" at a function organised by a college here in Maharashtra, General Naravane said national security was not limited to Armed Security only but is based on six other important foundations. Speaking about non-traditional threats to National Security, General Naravane said, "Info security is the biggest challenge to our national security in the present scenario" "Cyber warfare is one of the non-traditional threats, it is not the only threat to our information system, but it is also a threat to leaking of sensitive information of our country," Army chief said.

Reference : https://timesofindia.indiatimes.com/india/info-security-biggest-challenge-to-national-security-army-chief/articleshow/80426626.cms)

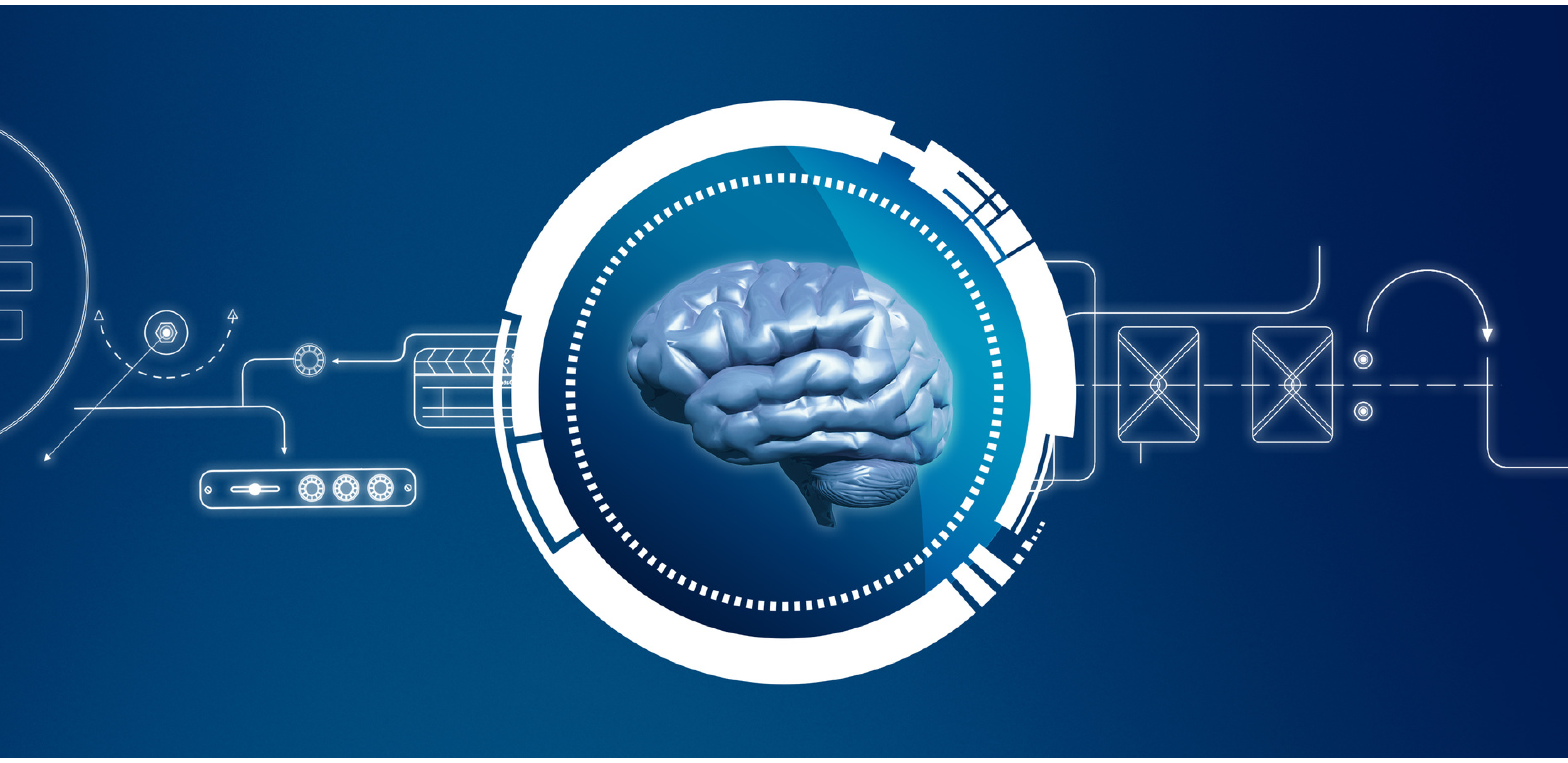
IMPACT OF CYBER CRIMES ON NATIONAL SECURITY

Cyber Crime continues to grow & challenge developed countries different methods. Information available on cybercrime can be found at periodic reports on consultation, IT and information security companies, and law enforcement agencies. Given the problems that exist in identification feasibility, ineffective use of numerical mathematical methods analysis, and the inclusion of indirect damage in financial audits, it is clear that the available information is not reliable. It seems like money Testing is constantly increasing. Still, there is a big deal the potential danger of cybercrime is overlooked. An analysis of some article shows that it is actually a huge list of cybercrimes does not represent a threat to national security. Phenomena such as theft and industrial spying, fraud, harmful content, hate Crime, website vandalism, denial of service, and so on are responsible for it become a National Security issue only if there is a significant increase their events and their consequences are permanent. So, now is the time to take action to reduce the risk and make it more difficult for cyber criminals working in this area.



BRAIN COMPUTER INTERFACES

BRAIN COMPUTING INTERFACE



Brain Computing Interface is also called Brain machine Interface (BMI) is a direct transmission track between the brain's electrical activity and an BCI device, most commonly Computer and Robot. BCI is a computer-based system which receives brain signals, (alpha, beta, gamma) analyses them and translates them into commands that are relayed to an output device to carry out a desired action. In assumption, any type of brain signal can be control through BCI device.

HISTORICAL BACKGROUND OF BCI

The history of brain computing interface was started in 1924 by Hans Berger, he discovered the electrical activity of the human brain and thus the development of electroencephalography (EEG). Hans Berger was the first psychiatrist to record human brain activity through EEG.

Berger was able to identify the brain waves, which are also called Berger's wave or alpha wave by analysing EEG traces. Berger examine the connections of alternations in his EEG wave diagrams with brain diseases.

In 1970 Jacques Vidal coined the term Brain computing interface, He was the pc scientist, in 1970s, He started research on BCI at the University of California, Los Angeles (UCLA) undergoing the acceptance from the National Science Foundation, followed by an agreement from DARPA. (The Defence Advanced Research Projects Agency (DARPA) could also be a research and development agency of the US, Department of Defence). In 1973 Jacques Vidal's paper marks was the first appearance of the expression on Brain Computing Interface in scientific literature. the foremost purpose to create BCI technology is for the folks that have lost their sensory motor function by neuromuscular disorders such as amyotrophic lateral sclerosis, cerebral palsy, stroke, or spinal cord injury. therefore, the goal of BCI is to exchange or restore useful function to the people disabled by neuromuscular disorders.

BCI works as prosthesis or prosthetic implant. Prosthetic implant may be a man-made device that replaces a missing part, which may be lost either from birth or by disorders. (The first neuroprosthetic devices implanted in humans appeared within the mid 1990's.)

IMPACTS OF BCI TECHNOLOGY ON OUR NATIONAL SECURITY, DEFENCE SYSTEM

The main purpose of the BCI technology is for the people who were disabled by neuromuscular disorders, but in this cyber world it became one of the cyber machines which connects to internet or Bluetooth, and it can operate all those devices which are connected to internet, e.g.: Internet of Things (IOT). All they have to do is to connect all IOT devices to BCI machine to operate without any physical activity, they can operate by brain signals, by just thinking or by giving commands. We can also see this type of technology in several movies, e.g.: In Avengers movie we can see that this type of technique has been used, and also in many of Hollywood movies, mainly in sci-fic. With BCI technology we can operate cars by brain command, The human brain produces electromagnetic signals. They can be measured using a special cap with 16 sensors (BCI machine). The measurements from the sensors can be interpreted as patterns by the computer. It can be done by connecting BCI to autonomous car. The car should be equipped with a variety of sensors and can be controlled by a computer.

*Case Study: They implemented two stages to test the usability of the BCI for controlling car. In the first stage the car was completely brain controlled, using four different brain patterns for steering and brake. In a second stage, decisions for path selection at intersections and forking's are made using the BCI. Between these points, the remaining autonomous functions (e.g., Path following and obstacle avoidance) were still active. They evaluated their approaches in a variety of experiments on a closed airfield. (Reference: Research paper written by Daniel Gohring, David Latotzky, Miao wang, and Raul Rojas, The Artificial Intelligence Group of Institute for Informatic, Free University Berlin, Germany)

BCI IN DEFENCE SECTOR

The U.S. Defence has already started using BCI technology, the Department of Defence (DoD) has invested in the development of technologies that allows the human brain to communicate directly with machines, including the development of implantable neural interfaces able to transfer data from the human brain to digital world. This also use to monitor a soldier's cognitive workload, and to control a drone. This could be very beneficiary to DoD, it can be use in defence tactics and now in this modern world wars are done by cyber technologies, which also includes Drone attacking and BCI technology. It may become easy to control enemy's drones by getting access to them, if they come for an attack. Further technology can support soldier to soldier communication, performance monitoring and training; However, the policies, safety, legal, and ethical issues should be solved before this technology vastly come into the force.

In Defence sector BCI can be useful for future military operations and the BCI applications would support ongoing Defence technological initiatives, including human machine collaboration to improve decision making, and it can assist human operations and performance monitoring and training. They can also operate any drone by BCI technology. Precautions will need to be taken to Defence operations and institutions and to reduce potential ethical and legal risks associated with Defence development and adoption of BCI technologies.

Brain Computing Interface is the great invention, which was just tend to use as prosthetic implantation in earlier years, but now in this 21st century BCI has become more valuable device and has also become a cyber device which can be used in multiple ways, every electronic device or we can say every cyber device can be operated by BCI machine. BCI machine can be used by anyone, knowing that it has not remained just for the people who are disabled and we can buy it at very cheap price. BCI works by brain signals which are; Alpha, Beta, Gamma, and Tithe, this four signals converts into nine different combinations through which BCI machine can operate IOT, All we have to do is to connect Bluetooth to all those devices which we want to operate by BCI and have to concentrate properly without distracting to any other things because the brain signals which are going to produce combinations depends on proper brain concentration, and It is also a dangerous device when it comes to use in wrong way, BCI can take place in violent acts, like anyone can take access to any IOT devices through BCI machine and can operate it, It has become easy for hackers to gain access to IOT devices without knowing anyone. In cyber world it will be the new way of attack to the targeted people, it will become very difficult to recognise that the type of attack was BCI and also hard to recognise the cyber attacker. Now a days, there are many latest vehicles which has automatic functioning means the car can be driven by commands without using any BCI technology, but this type of cars can be hacked by cyber attackers by using BCI machines, this can be an advantage for them they can operate any autonomous car through BCI machine by being in its range, it means a ongoing vehicle can also be hacked and the criminals can take control on it which can be very dangerous, it can take place to violent act, and hard to recognise hacker and the technique used by them. Now, world has developing very vastly in which cyber is one of the reasons, there are many new technologies which were introduced to the world by several countries and so many people working on ongoing project and also there are so many new technologies yet to produce and introduce to world, and also there are almost all human organs are making by laboratories in which BCI may use, seeing to this fast development in future it could be possible that human will turn into Cyborg. A person could be considered as Cyborg when they are outfitted with implants such as artificial organs, and a person could also consider as Cyborg when they use wearable technologies like google glass or using laptops or any cyber devices to do work. That is why, it is absolutely right to say that we are living in Cyber World.

DRONE TECHNOLOGY & INTELLIGENCE SURVEILLANCE

DRONE TECHNOLOGY & INTELLIGENCE SURVEILLANCE

Introduction : In the era of developing world the globalisation goes in advancement in each and every terms as the countries are moving to development the race to sustain remains constant as there is a race it brings the competition for which there are rising threats to security not limiting to traditional (land or air) so to give a keen look to this aspects drones are the essential bodies who can give easy access to scrutiny non-traditional security challenges.

A Drone may be a flying robot that can be remotely controlled or fly autonomously using software-controlled flight plans in its embedded systems, that employment in conjunction with onboard sensors and a worldwide Positioning System (GPS). Drones now have many functions, ranging from monitoring global climate change to carrying out search operations after natural disasters, photography, filming, and delivering goods. And also, Drones can go places that humans can't access, in order that they are an ideal solution for dangerous search and rescue efforts, also as for delivering emergency supplies to remote locations and disaster areas. But they're most well known as controversial use by the military for reconnaissance, surveillance and targeted attacks.

Drones are pertaining to an unpiloted aircraft, another term for drones is an unmanned aerial

vehicle (UAV). And these drones don't require rest, enabling them to fly as long as there's fuel or power charging within the aircraft and there are no mechanical difficulties in this drone; Basically, these drones are employed by military purposes because they don't want to risk a pilot's life in combat zones.

The U.S. Navy was developing "air torpedoes" during war I, but put aside the concept until war II. At the time of war II, the Navy began an operation named Operation Anvil, during which remote controlled B-24 bombers were used to deliver explosives to German bunkers, many planes crashed or exploded. for many years afterward, the U.S. focused on using rockets

while also performing on drone development. the primary big demonstration of drones came during the 1991 Gulf War, when the U.S. deployed UAVs.

DRONES FOR NATIONAL SECURITY AND DEFENCE SYSTEM

In 2010, the **U.S Department of Defence** launched the spacecraft named The Boeing X-37, also referred to as the Orbital Test Vehicle, may be a reusable robotic spacecraft. it's boosted into space by a launch vehicle, then re-enters Earth's atmosphere and lands as a spaceplane. The X-37 began as a NASA project in 1999, before being transferred to the us Department of Defence in 2004. The X-37 is operated by the us Space Force, and was previously operated by Air Force Space Command until 2019 for orbital spaceflight missions intended to demonstrate reusable space technologies. The X-37B unmanned spaceplane is shrouded in mystery. With its bullet liked shape, stubby wings, and a couple of tone black and white appearance, and it's like a smaller, cuter version of the manned orbiter that served NASA for many years. The Drone in space is that the U.S. military's mysterious X-37B spacecraft, which has made multiple flights in to orbit for many days at a time. There are multiple sorts of Drones were produced in which Drones have many different categories to use for Defence and Homeland Security. In Defence and Homeland Security, Drones are often use as Anti-Terror, Border Security, Counter Insurgency, Crime Control, Crowd Monitoring, Disaster Management, Forest & Wildlife, & Traffic Monitoring.

An Indian Overview for Drones : at the present The Indian Government is focusing on Drones (Unmanned Aerial System) which visiting be a transformative technology compared with internet, GPS. Large corporates have made investment for Drones systems during which 200+ drones were beginning to be produced in India, strong academic researchers also being encouraged for Drones researches, Countering Rogue Drones (C-UAS) are prevailing geopolitical & security environment. Several sensitive and critical infrastructure sites in government and private sector require CUAS, especially with increasing ubiquity of drones in civilian space and they need to track every drone with Remote ID and Unmanned Traffic Management (UTM).

Drone Rules 2021 : Indian Drone Policies and Landmark Turnaround in 2021, Proactive regulatory environment (Drone rules 2021) has led to a significant increase in market opportunity. On 7 Oct 2014 Directorate General of Civil Aviation (DGCA) issued a public notice in which they given prohibiting use of Remotely Piloted Aircraft System (RPAS) for civil applications. After 3 years in Nov 2017, DGCA car (draft) requested for operation of Civil RPAS. In Aug 2018, DGCA car (w.e.f. 1 Dec 2018) requested for operation of Civil RPAS. Later in June 2020, Draft UAS Rules 2020 were published and On 2 Oct 2020 live Digital Sky Phase 1 were shown, and On Nov 2020 National UTM policy draft were discussed, In 2021 on 12 March, Notification for UAS rules 2021 were released and On 25 Aug 2021, Notification of Drone rules 2021 were released, and within a month on 15Aug 2021 Production Linked Incentive (PLI) scheme for Drones were released, On 25 Sep 2021 Airspace Maps were released and on 24 Oct 2021 National UTM Policy were released. World's Largest Drone Project in India by doing Survey of Villages Abadi and Mapping with Improvised Technology in Village Areas (SVAMITVA), which has impact on 950+ million people in rural India. The project has started from 24th April 2020, in which they did Mapping of 662,000 Indian villages, in which 2+ million square kilometres of aerial imagery were taken and Drones based surveys carried out in ~100,000 villages in almost all states, through this survey up to 3,668,767 Property cards were issued as of 18 Jan 2022. Benefits delivered through this survey: - 1) Financial stability and access to loans. 2) Accurate land records. 3) Property tax determination. 4) Multi use GIS maps. 5) Better GPS Development Plan. 6) Reduce property related disputes. Drones are an enabling societal impact technology delivering value across multiple sectors, proven by the success of SVAMITVA scheme. Vision 2030 for Drone Industry in India: To make India the Drone Hub of the world by 2030, offering most competitive and innovative manufacturing capabilities.

Mission : Achieve manufacturing potential of INR 180,000 crore (US$ 24 billion) by 2030. Sectors Covered: 1) Defence: Indian Army, Indian Navy, Indian Air Force. 2) Commercial: Infrastructure, Retail, Agriculture. 3) Homeland Security (HLS): State Police, Paramilitary Forces. 4) Counter-UAS.

Global Drone Market Trends : Defence remains Biggest Segment in which Drones have played a key role in the Defence sector for the past 5 decades with Israel and USA leading the R&D efforts. Drones have historically represented approximately 3.5% of U.S. Air force and Navy procurement spending. This ratio is anticipated to increase by 0.25% each year as autonomous aircraft plays larger roles in future engagements. Defence will remain the largest segment until 2024, Enterprise will become the largest after 2024. The global drone economy was $15 billion in earlier years which was worth about $20 billion in 2018, according to a global forecast published in researchandmarkets.com. It is expected that the global drone's economy will grow from $20 billion to $90 billion till 2030.

As of 2020, Drones for Defence market share is larger than all other segments combined. Enterprise segment is growing rapidly and will take the lead by 2025. However, by 2030, It has expected that Logistics alone to become the largest growth.

Statements by some officials, from FICCI Session on Drones & Counter Drone Opportunities in Defence and Homeland Security at Aero India.

Mr. Rakesh Asthana (Director General, Border Security Force) : Pakistan using drones for surveillance, smuggling arms, explosives and narcotics 77 incidents were done in 2020, Indian Government has already authorized sizeable number of UAVs for the BSF, and also 10 counter drones were approved by Ministry of Home Affairs.

Brig. ZIS Yazdani, SM, VSM (Army Design Bureau, Indian Army) : Requirement of Drones in high altitude areas for surveillance and logistics, Indian Armed Forces asking for more UAVs with better technology and longer range, hale being procured with a ceiling of above 40,000 feet with a range of 5000 kms. Strong case being developed for a runway independent RPA which can go at least 200 kms inside, exploring medium range precision kill system with a range of 40-60 kms and loitering munitions, and also looking for C-UAS with detection, jamming & spoofing and all integrated into one.

Mr. M.A. Ganapathy, IPS (Director General, Bureau of Civil Aviation Security) : Technical specifications for counter drone solutions issued so that all airport operators can install such solution. BCAS has informed stakeholders, especially airport operators to install counter drones and BCAS is in the process of issuing new dates to airport operators for installing counter drone solutions.

(**Reference : FICCI Session on Drones & Counter Drone Opportunities in Defence and Homeland Security at Aero India Show 2021**)

Statements by Key Leaders

Hon'ble Defence Minister inaugural address at Aero India Feb2021

Vision to make India one of the biggest countries in Defence Sector, Target turnover of Rs 1,75,000 Crore in Aerospace and Defence by 2024, India is steadily marching from 'Making in India' towards 'Make for the World', India holds a huge potential for investments in the aerospace sector.

Hon'ble Army Chief Gen MM Naravane's address at USI Aug 2021

Technology is impacting nature & character of war, will influence doctrines, concepts, Tech platforms will help bridge military asymmetries, need to transform our game in accordance with adversaries renewed capabilities and Indian Army is engaging & supporting start-ups, technology institutions. Drones For National Security Ecosystem, in which Army, Air Force, Navy & Coast Guard, Border Security Force, Paramilitary Force, Intelligence Services, State Police Forces, and including Defence Production, every system uses this drone in different ways. a) Army uses drones for several things like, intelligence, Surveillance &Reconnaissance (ISR) of targeted areas, carry out night patrols, drones give combat support to infantry units, perform short range, quick look reconnaissance missions, Perimeter surveillance of army bases & cantonments, Target destruction, including use of drones and provide communication network to units in remote areas, and broadcasting information in critical areas. b) Navy & Coast Guard, performs ISR missions and uses for Port security and Naval bases, it helps in logistics support between ships and monitor, track, & inspect vessel movements and assist in navigation and maritime traffic management at ports. c) Air Force, uses for Imagery Intelligence gathering and reconnaissance, also uses for Air support to combat missions and perimeter surveillance for Air Force bases and Autonomous, attractable for loyal wingmen. d) Border Security Forces, uses the drone technology for Aerial border surveillance, monitor suspicious activities at night patrolling and provide combat support and medical assistance to deployed units. e) Paramilitary Forces, performs ISR activities, provides combat support to field units and also keep 24 hours aerial patrols, track persons of interest and support disaster relief. f) Intelligence services, stealth intelligence mission through drones and continuous monitor and track the person of interest and provide air support for offensive intelligence operations. g) State Police Forces uses the drones for monitoring crowd & Surveillance and for public broadcast and they track & monitor anti-social elements specially in night patrolling to search and rescue. h) Defence Production, in defence production their work uses drones for project monitoring, Aerial inspections, inventory management and for Security & surveillance of sites

TYPES OF DRONES AND THEIR USES

In this era, every impossible things are trying to make possible through modern techniques and new inventions, In which one of the invention is Drones technology, which are most well known as controversial use by the military, it's not just about Defence and Intelligence surveillance, this inventions is made for several other sectors also, e.g. Enterprises, Drones have becomes an important part in operations such as mapping, surveying, equipment inspection, project monitoring and precision agriculture activities. It also uses in Construction & Real Estate, Industrial Asset Inspection, Mining, Oil & Gas, Power Transmission, Solar Energy, Wind Energy. The disposal of drones for such operations decreases crew costs by reducing time consuming ground observations. In Defence and Homeland Security, Drones use as,

1) Anti-terror to detect threats and identify risk prone areas from a remote location.
2) Border Security for conducting reconnaissance missions and track illegal activities without risking lives.
3) Counter Insurgency for conducting surveillance and gather actionable intelligence.
4) Crime Control to Enhance law enforcement with remote situation assessment and crime scene analysis.

5) Crowd Monitoring to Detect irregular activity and gain in depth situational awareness.
6) Disaster Management uses to gain real time knowledge of the situation and plan search and rescue operations effectively.
7) Forest & Wildlife uses to track criminal activities and boost conservation efforts.
8) Traffic Monitoring to analyse and control traffic movement and respond to emergencies more effectively. Certain companies are considering sending drones to deliver goods, which could reduce the cost of using drivers for door-to-door services, Amazon is planning to deliver their parcels via drones to clients in just 30 minutes or less. The company has drafted a letter of request to the FAA to start this service. Amazon had performed its first drone deliveries in Britain in December 2016.

Prime Minister of India, Narendra Modi ji focus on societal impact of drones has been key to the rapid growth of this nascent sector, we have to become a leading country in Drone Technology say's PM Modi, " We are engaged in providing digital records of their homes and land to millions of people by mapping them with drones in more than 600000 villages of India. This digital record is facilitating the access of people to access to credit and bank loans, while reducing property disputes.

"**PM Modi's address at United Nations General Assembly, 25th Sep 2021**" Drones are the topic which influence the creative power of our Nation, especially in our youngster, India is one of the first countries in the world that is preparing digital land records in its villages with help of drones !

"**PM Modi's Mann ki Baat broadcast, 24th Oct 2021"** New drone rules will open avenues for innovation, Business in India. Empowering Farmers across India with Hundreds of Drones named 'Kisan Drones'. Glad to have witnessed Kisan Drones in action at 100 places across the country on 19 Feb 2022”.

Indian Army is using Drones to supply booster doses of covid vaccine to forward troops in snow bound areas of Jammu & Kashmir, The supplies are delivered to inaccessible areas with the help of drones as a part of mission Sanjeevani. In this case, the package is dropped as line-of sight issues do not accept it to land or come lower. Package was well padded for protection. The process is divided into 3 stages: Initial briefing by RMO, preparing of dropping zone & suspension of the payload, In the first stage, The Officers are being briefed about the delivery process of the supplies. In 2nd Stage, Officers can be seen cleaning the drones' Take off and deliver zones. In 3rd Stage, the package is then attached to the drone which travels to the designated area. The Package is then dropped to the ground in the presence of an officer who is waiting in the area. The Indian Army also said that the packages are well padded for protection so there is no damage.

(Reference : Hindustan Times and Indian Army shared the video of the entire delivery process on social media.)

GOVERNMENT BUDGET TOWARDS DRONES

Drones are not just uses for military purposes but it also uses in several different ways like, Wildcraft photography, Video creator, Farming and nowadays it is also using in weeding's. With this vest use of drones, it automatically became, one of the cyber threats because it also connects to internet, it can be operated by mobile phone by connecting to internet through some drone operating applications. Total addressable market potential for drones in India, till 2025 is 77,300 Cr, in which it covers C-UAS, Defence, Commercial, HLS, and Exports budget will gone be 4,300 Cr, means totally 81,600 Cr for market potential of drones, and it is expected to turn 2,95,000 Cr including exports till 2030.

This is a very vest investment for drones done by Indian Government and that is why; it is really mandatory to take proper precautions against Défense operations and institutions and to reduce potential ethical and legal risks associated with Défense development and in all sectors because, any gadget, once it becomes a cyber threat it also becomes new attacking threat for hackers or cyber attackers, Drones can be hacked by hacker or on war field it can be hack by opponents' forces. Drones can hack by several hacking tools, but it also can hack by BCI (Brain Computing Interface) gadget, by connecting with Bluetooth or WIFI, nowadays, it is really easy to take access to any cyber devices, so before using any cyber devices, it is mandatory to take proper precautions about those devices, and also precautions will need to be taken to defence operations and institutions to reduce potential ethical and legal risks associated with defence development and in all sectors.

DATELINES OF CYBERCRIMES

1939 MILITARY CODE BREAKING

Alan Turing and Gordon Welshmen develop BOMBE, an electro-mechanical machine, during WWII while working as codebreakers at Bletchley Park. It helps to break the German Enigma codes.

1984 US SECRET SERVICE

The U.S. Comprehensive Crime Control Act gives Secret Service jurisdiction over computer fraud.

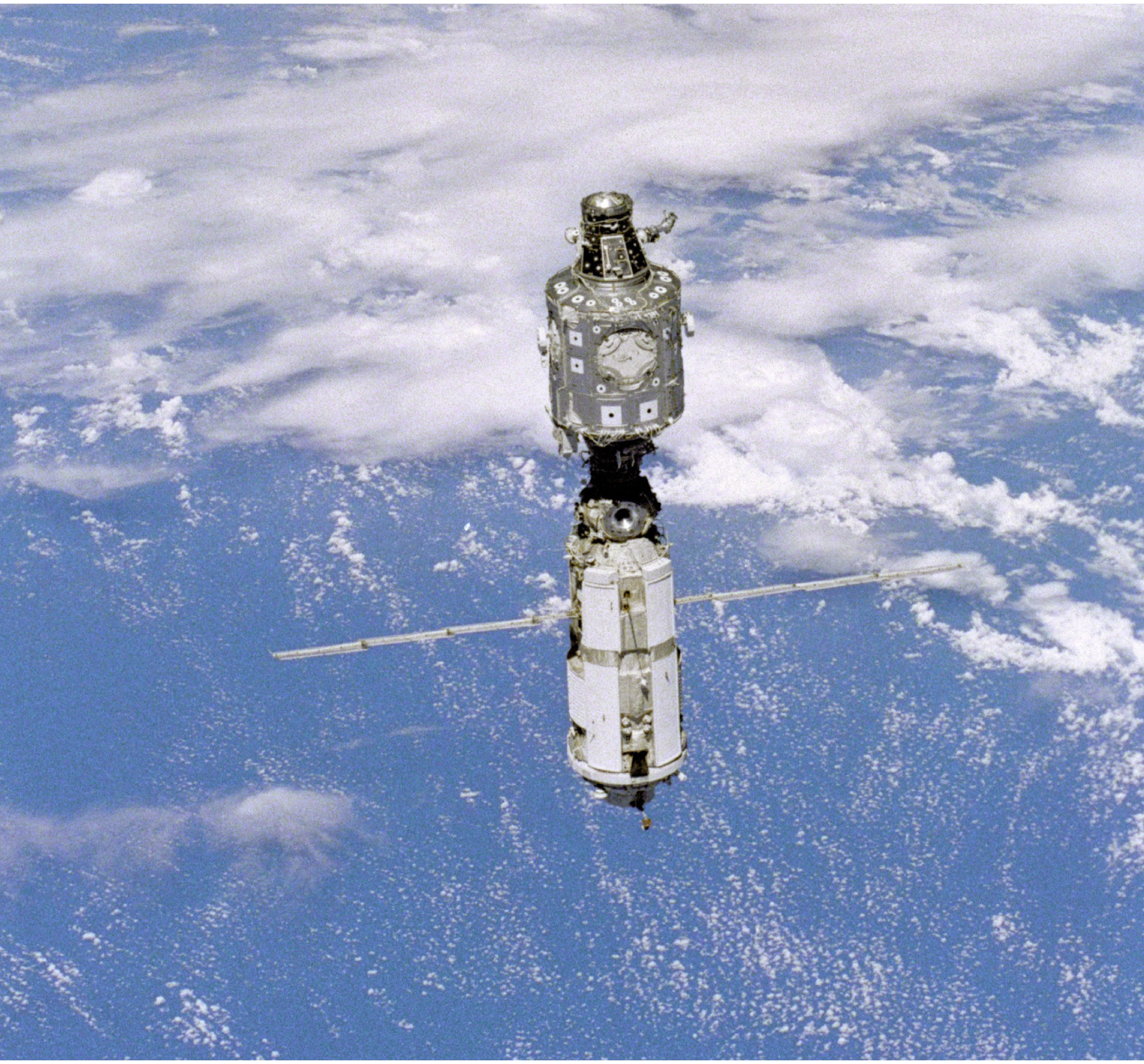
1989 TROJAN HORSE SOFTWARE

A diskette claiming to be a database of AIDS information is mailed to thousands of AIDS researchers and subscribers to a UK computer magazine. It contains a Trojan (after the Trojan Horse of Greek mythology), or destructive program masquerading as a benign application.

1994 DATASTREAM COWBOY & KUJI

Administrators at the Rome Air Development Centre, a U.S. Air Force research facility, discover a password "sniffer" has been installed onto their network, compromising more than 100 user accounts. Investigators determined that two hackers, known as Data Stream Cowboy and Kuji, are behind the attack.

1999 NASA & DEFENCE DEPARTMENT HACK



Jonathan James, 15, manages to penetrate U.S. Department of Defence division computers and install a backdoor on its servers, allowing him to intercept thousands of internal emails from different government organizations, including ones containing usernames and passwords for various military computers. Using the info, he steals a piece of NASA software. Systems are shut down for three weeks.

BIBLIOGRAPHY

1.https://timesofindia.indiatimes.com/india/info-security-biggest-challenge-to-national-security-army-chief/articleshow/80426626.cms

2.https://www.inss.org.il/wp-content/uploads/sites/2/systemfiles/SystemFiles/MASA4-3Engd_Tabansky.pdf

3.Attended an online webinar lecture, In which Mr. Rajan Luthra Sir (Head- special projects, chairman's office and chair, FICCI committee on Drones, Working as Group leader and Co-Author, in Reliance Industries Ltd.) were addressed.

4.Hindustan Times and Indian Army shared the video of the entire delivery process on social media.

5.FICCI Session on Drones & Counter Drone Opportunities in Defence and Homeland Security at Aero India Show 2021

6.https://www.herjavecgroup.com/history-of-cybercrime/

CYBER DEFENCE

CONCEPT BY

DOCTOR
TANMAY S DIKSHIT

FORWARD BY

BRIGADIER
HEMANT MAHAJAN

EFFECTS OF CYBER SECURITY ON THE MILITARY & NATIONAL SECURITY

AUTHOR - SHIVKUMAR BALRAJ NILI