International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

The Inevitable Menace of Cyber-Warfare: A War by the Computer & for the Computer

Prashant Dutta[1], Pranay Dutta[2], Pradeep Pillai[3]

[1]Manager-IT, MPPKVVCL, Jabalpur
[2]Senior Staff Engineer, Intercontinental exchange
[3]Associate Director, Cognizant Technology Solutions

Abstract:
The future wars shall not be fought on Land, probably no bullets shall be fired, it will be fought in the Cyber Space, and it will be fought through the Internet or the Dark Web. Espionage will not be done by spies on enemy soils, but now it will done virtually on enemy data through cyber space. Radar stations will not be bombed anymore, but they will be jammed/hacked. Bridges and ammunition depots will not be targeted anymore, but the Data Centers will be targeted. The aforementioned cataclysm is the prediction of new age warfare- "The Cyber Warfare". The aim of this paper is to bring forth the devastating capabilities of the Cyber Warfare. Also this paper aims to point the techniques which may be used to inflict wounds on enemy data/communication along with the loop holes present and finally finding ways to avert these clear and future dangers.

Keywords: - Espionage, Hacking, Server, IoT, Cloud, Firewall, Anti-Virus, DDoS, Cyber security

1. Introduction

Before going any further, it is pertinent to discuss how things are interconnected through internet, or how every device in the world can be reached from any other device located anywhere in the world . Some of the sectors which are highly IT dependent and connected over the Internet are as under:-

1. Banking and Finance (Online Banking)
2. Airports (Online Fleet Management and Ticket booking)
3. Railways (SCADA and Ticket booking)
4. Toll Gates (Fast Tags)
5. CCTV (Online Feed of CCTVs)
6. Mobile Phone (Apps like FB, Whatsapp, Insta, Location access, email etc)
7. Hospitals (Network Hospitals and non-network Hospitals store all the Data in the Cloud nowadays)
8. Electricity Department (The Grid is over the Internet)
9. Unique ID or other ID like Passport Data is also over the Internet
10. Land and Revenue data is also over the Internet

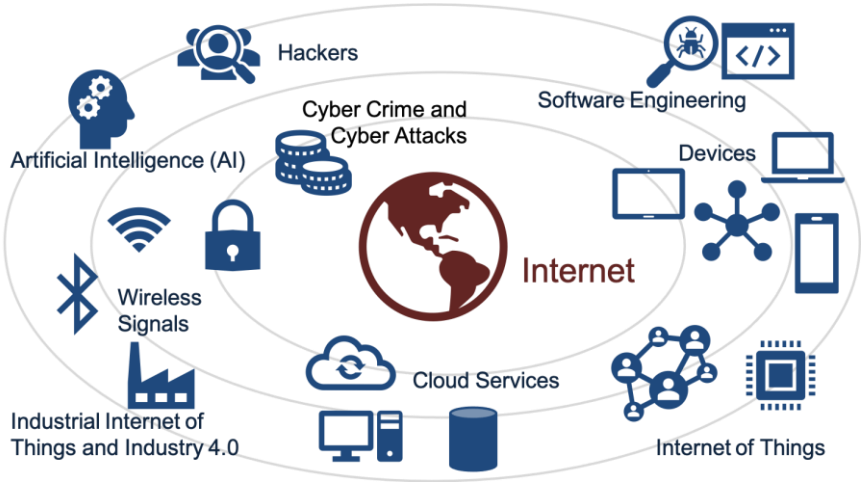

Fig 1.1 Cyber Space

1.1 Internet of Things :- The Internet of Things (IoT) has instigated novel challenges to the Cyber Security Domain. Previously only the Computers, Routers, phones were connected to the internet. But after the introduction of the IoT, all the worldly things are slowly getting connected over the Internet. We are living in an era where-in we can switch on the Air conditioner of our house by mobile phone simply sitting at the office, we can set the ignition "on" of our car even being seated kilometers away from the car. The aforesaid technological development has given a clear mandate to the Hackers to connect to any device in the world, which is connected over the internet. This means that if the "IoT" is being hacked then the world can be put into a total rampage beyond our comprehension.

How Does IoT Works, A Typical IoT System has mainly 4 Parts:

a) The IoT Enabled Smart Device
b) IoT Software/Firmware
c) GUI to access the Smart Device
d) Communication Channel (Typically the Internet)

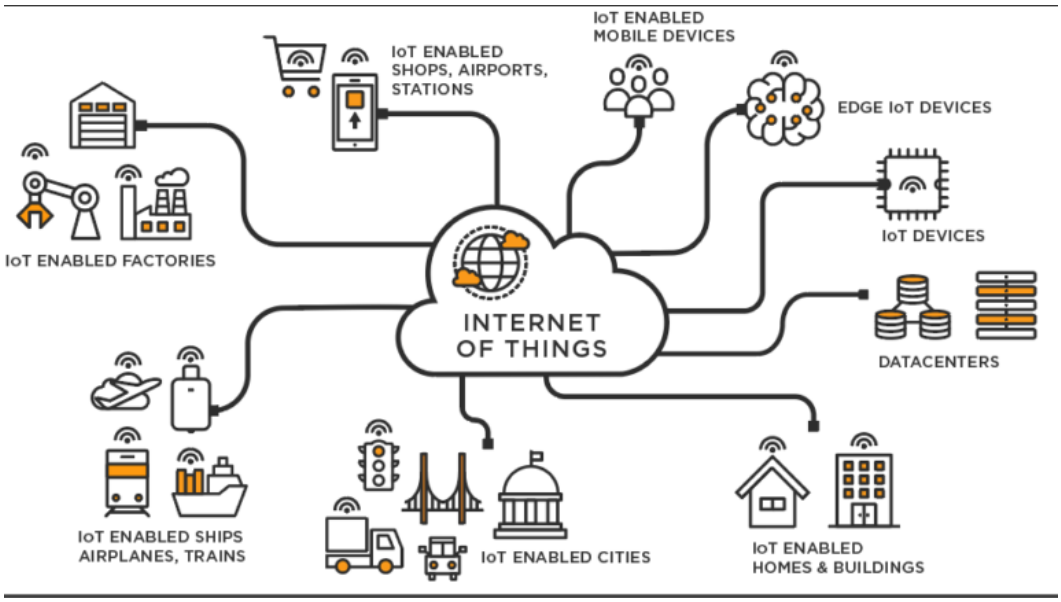

Fig 1.2 IoT

1.2 Data Center and Cloud - "A curse in disguise" for the Cyber world

Before the evolution of the Internet, the computers were decentralized hence were protected from the Cyber Threats. But after the dawn of the Internet all the devices connected over the internet are susceptible to Cyber Threats. Taking this further it can be said that Data Center or Clouds are actually "curse in disguise" for the Cyber world. Because now the data is stored centrally just like Money is stored centrally in bank and is more susceptible to robbery than money stored in the homes of individuals. The companies having their application running in the INTRANET through Local Data Center are less prone to cyber Threats than the companies which are storing Data in Cloud and accessing over the Internet.

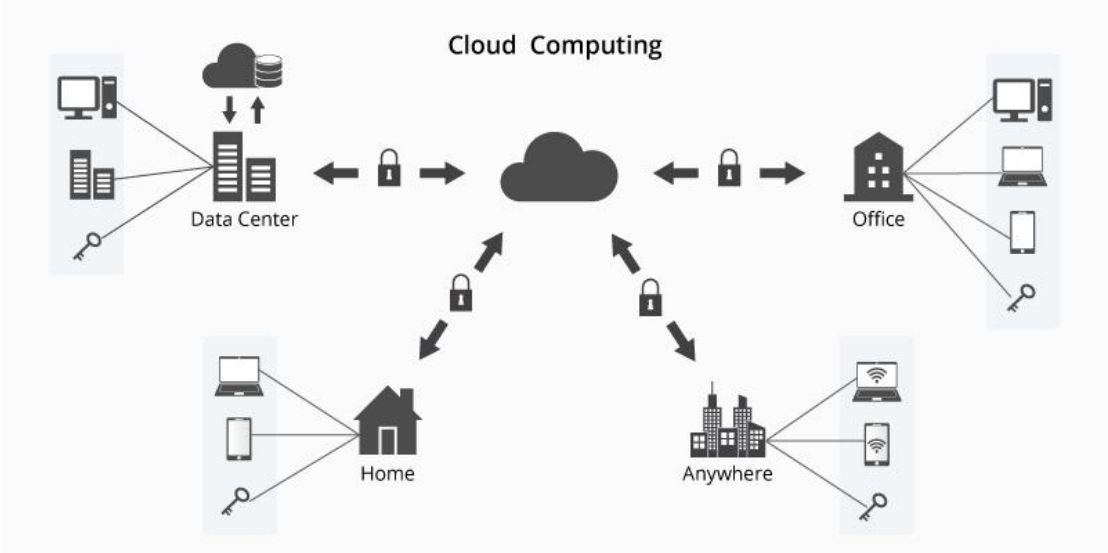

Fig 1.3 Cloud Computing

1.3 Cyber Warfare

The conventional techniques of war are going to become obsolete with the advent of Cyber Warfare. The war front will not be enemy ground but it will be enemy data center and servers. The Cyber war will be fought at novel fronts like:-

a) Espionage:

Espionage in future will be grossly different with respect to what it is now. Espionage will now not be limited into military affairs but it will progress leaps and bounds into different paradigms like Industrial/Trade espionage, Online Elections/Electronic Elections etc. Nowadays almost all organization has thousand of chat group within them, and probably all the info about that organization is some or the other way discussed through these chat group or emails. For the spies who are lurking for data, these chat groups / email shall be feeding frenzy.

b) Sabotage:

Cyber Sabotage disrupts the usual working of a Software System and kind of highjack's the system and compels it to perform malicious behavior.

c) Denial of Service Attack:

A 'denial of service' (DoS) attack involves overcrowding a website with fake-requests, hence the processing speed of the site reaches to its max limits thereby it hangs the system and the site crashes down.

Application-layer attacks – Also known as layer 7 (L7) attacks. Common L7 DDoS attacks include Slowloris, Slow POST, HTTP flood attacks, and Challenger Collapsar (CC).
Protocol attacks – Sometimes called computational or network attacks. Common protocol attacks include SYN flood, Ping-of-Death, and Smurf
Volumetric attacks – Also known as floods. Common volumetric attacks include User Datagram Protocol (UDP) and ICMP flood (or ping flood).

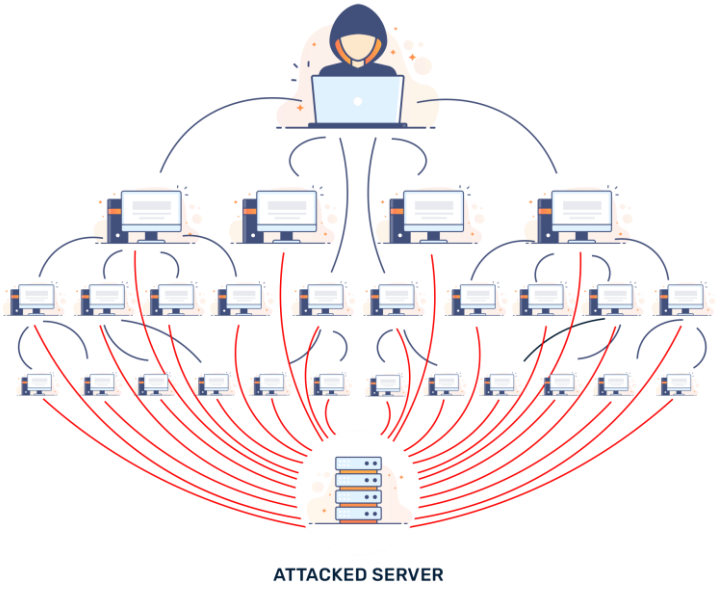

Fig 1.4 DDoS

d) Electrical Power Grid

The Electrical department like other departments are completely IT Enabled. The SCADA system (supervisory control and data acquisition) enables to control electrical equipments from the internet. Hence they are prone to hacking. Hijacking the power-grid could give enemy the ability to immobilize critical systems, disabling infrastructure and lead to deaths of many lives. It can also interrupt communications.

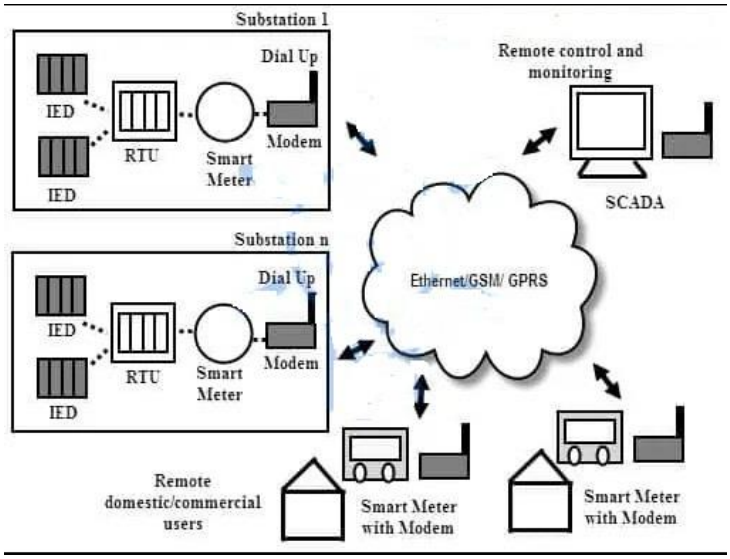

Fig 1.5 SCADA System

e) Propaganda

Propaganda war is the new war run by enemy states to spread the false narrative for the targeting nation via social media etc.

f) Economic Disruption

The functioning of the economy system is completely IT Enabled nowadays. Attacking the computer networks of financial sectors like stock-markets, payment-systems, or banks can give hackers entrée to funds or put a stop to their targets from getting the finances they need to thrive.

g) Surprise Cyber attack

These refer to the type of cyber attacks that could have an impact similar to Pearl-Harbor or '9/11'—attacks take the enemy on surprise by waning their defence. They can be used to wane the enemy in preparation for a physical-attack as a form of hybrid-warfare.

h) Communications disruption

Emails, Phones/mobiles or other kind of communication network could be hacked/tampered/intercepted and thereby disrupting the entire communication network.

i) SQL injection

attacks involve inserting malicious code/virus into Software's database through a flaw in the software's input-validation process.

j) Supply chain attacks

involve confronting a company/organization's supply-chain to get access to its software or data.

k) Crypto Jacking

Crypto Jacking refers to manipulating Crypto Currency by taking control on the Crypto Algorithms.

l) Zero Day Exploit

A Zero Day Exploit occurs after the declaration of network susceptibility; there is no resolution for the susceptibility in most of the cases. Hence the dealer notifies the susceptibility so that the users are alert; though, this information also reaches the invaders.

m) Watering-Hole Attack

The sufferer here is a picky group of an association. In such an assault, the attacker targets portals which are regularly used by the targeted-group.

n) Domain Name System (DNS)Tunneling

Hackers use the DNS to evade safety measures and talk with a remote-server. DNS tunneling is a type of hack attack using the Trojan horse technique where hackers embed malicious-code into a MSG that looks like a DNS-request. Since DNS is an important part of most network & internet, this sort of traffic is seldom able to bypass through firewalls and UTMs without much analysis.

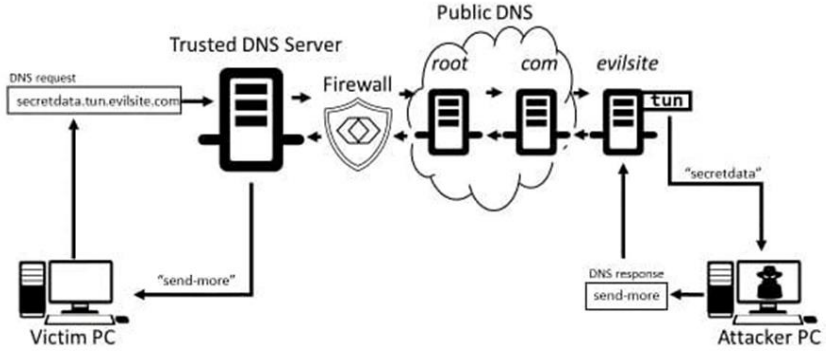

Fig 1.6 DNS Tunneling

o) DNS Spoofing

Cyber attack in which a hacker manipulates the DNS account from a Portal to direct its traffic.

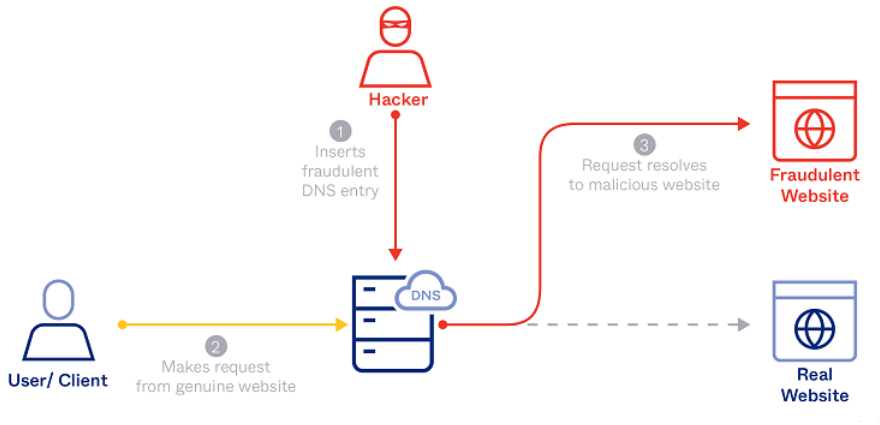

Fig 1.7 DNS Spoofing

p) Cross-site scripting (XSS)

is an assault in which an hacker injects malicious ".exe scripts" into the code of a trusted-application or Portal. Hackers often set off an XSS-attack by sending a 'malicious link' to a user and tempting the user to click-it.

q) IP spoofing

IP spoofing is a sort of malevolent attack where the hacker hides the true-source of IP-packets to make it tricky to know their origin. The hacker generates packets, altering the origin IP address to imitate a different system, masquerade the sender's individuality or both. The spoofed packet header-field for the source IP-address contain an address which is different from the real source IP-address.

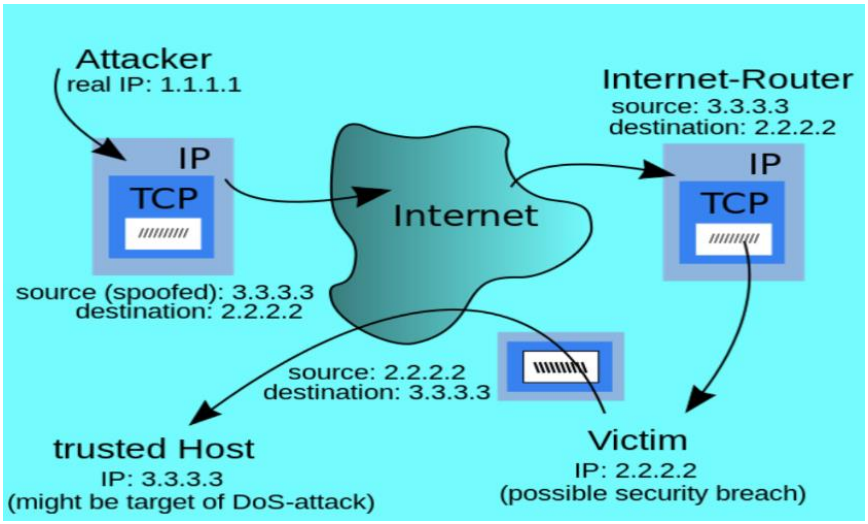

Fig 1.8 IP Spoofing

r) ATM Cash Dispensing

Hackers use the bank ATM in a fraud manner to dispense money

s) Whale Phishing Attacks

In this the hackers target high profile persons using classy social-engineering system to get insightful information.

t) URL Interpretation

By manipulating some sections of a URL, a hacker can get a web-server to render web-pages that they are not allowed to have access to.

"http://target/forum/?cat=**********"

u) Session Hijacking

The hacker gets right of entry to a user's session-ID to validate the user's session with a web application and overtake the user's session.

v) Brute Force Attack

A hacker gets illegal access to a system by trying a variety of passwords until the right one is found. It can be very effectual against weak-passwords.

2. Forms of plausible Cyber Attacks Suggested through this Paper

2.1 UPI Phishing –

The digital transformation has introduced the digital money and various UPI based apps are available in the market for sending and receiving money. The UPI accounts for more than 50% of Digital transactions in India in that case phishing through UPI can disrupt the economy. UPI Phishing can be executed by using the following Techniques:

- Phone Cloning
- Taking phone of Remote(AnyDesk for example)
- OTP based frauds
- Malware based frauds- by making you to click on any fake link
- Installing malicious Apps
- Using Open Wifi can be susceptible to hacking
- Using Duplicate QR Code above an original QR code

2.2 Hacking the SCADA systems –

The Railways use SCADA for Traction control and the Electrical Discoms use SCADA to control the Feeders/DTRs etc. Hacking this SCADA system means disrupting Electricity Power Distribution and disrupting Railway Traffic Management.

2.3 Hacking the Public Service systems –

Many public service systems are automated nowadays like Traffic Signals, online bill payment of municipalities, online land record systems, online customer care systems. If the above are hacked then there will be chaos in between the local public.

2.4 Hacking a Video Conferencing –

Nowadays almost all organizations hold their meetings over Video Conferencing, in that case hacking a VC means getting all the info about the meeting.

2.5 Deep Fake –

A video or Photo which has been deliberately tainted and manipulated to feign a celebrity as doing or saying something which was not really done or said.

2.6 Hacking Military Communication network/ Military Database/ Radar Networks/ Satellites/ GPS/ ATC /AWACS

a) Satellite Hack-

To hijack satellite DVB-S links, one needs the following:

- A satellite 'Dish'—the dimension depends on geographical location and satellite

- A low noise block down converter LNB
- A devoted DVB-S tuner (PCIe card)
- A Computer, if possible running Linux

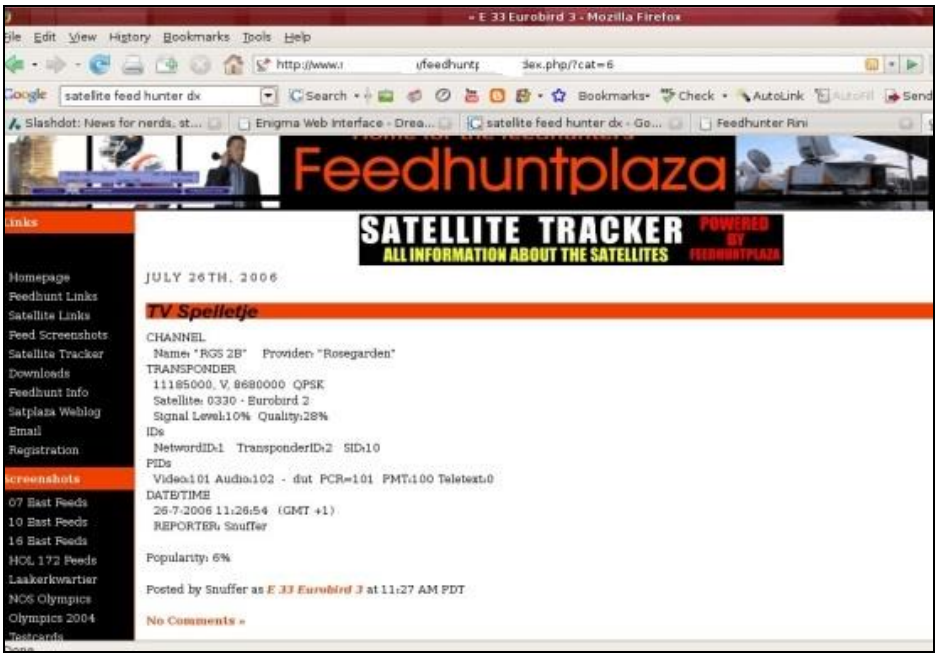

Fig 2.1 Satellite Hack[1]

Fig 2.2 Satellite Hack[2]

The countries defence sector solely depends on its indigenously built satellites for communication. If the satellites are hacked then military communication is compromised. For example In India GSAT series satellites are the defence force multipliers and provide communication to UAVs and AEW&C (airborne early warning and control aircraft) NETRA. Currently, India has only two devoted defence satellites — the GSAT-7 (Rukmini) and GSAT-7A (Angry Bird) — used by the Navy and Air-Force, respectively. The Indian Army has been reliant on GSAT-7A and other surveillance satellites like RISAT 2BR1 imaging satellite for communication and surveillance operations. With this approval for a military-grade satellite, the Army will get a new "eye in the sky' in getting fail-safe communication support.

Electromagnetic Intelligence Gathering Satellite (EMISAT), developed by ISRO has an Electronic Intelligence (ELINT) package called Kautilya, which allows the interception of ground-based radar and also carries out electronic surveillance across India.

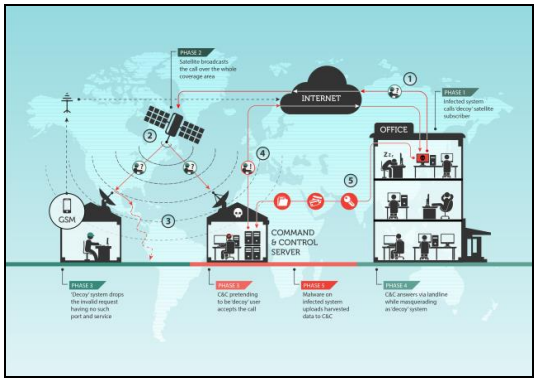

Fig 2.3

b) Hacking Missiles & Smart Bombs –

Missile launches depend on the way in which info is transmitted to the missile-launch-facilities and the way in which info is transmitted to the missiles in flight. There are many ways an offensive cyber attack against missile systems be launched. These include exploiting missile designs, changing software or firmware, or creating clandestine pathways to the missile command and control systems. The missile systems use computers and so they are, indeed, all vulnerable to cyber attacks.

There are rumors that USA hacked one of the Test Ballistic Missiles of North Korea and averted its launch. Similarly Smart bombs are GPS guided bombs and the information of the target is fed at real time by the fighter pilot so any breach of communication may lead to feeding wrong coordinates in the bomb and misguiding the same. An elite group of North Korean hackers secretly breached computer networks at a major Russian missile developer for at least five months last year, according to technical evidence reviewed by Reuters and analysis by security researchers.

c) Hacking Submarine Communication and Aqua-Fi –

One of the strongest in the Nuclear Triads is the Submarine. The Nuclear Submarine carrying their Nuclear Ballistic Missiles are lurking deep inside the oceans and are ready to fire Nuclear weapons at anytime. But before firing they need to communicate from the command center and get the Green Signal. To communicate with the Command Center is the trickiest part and enemies are in constant pursuit to intercept these communications. Once these Communications are intercepted then the war is half won. During WWII the NAZIS developed a Cyrpto device called as the “ENIGMA” which left the ALLIED forces keep wondering for years. Aqua-Fi is the latest technology to communicate inside the waves, it uses Raspberry Pi 3b, they were able to build an IEEE 802.11-compliant wireless.

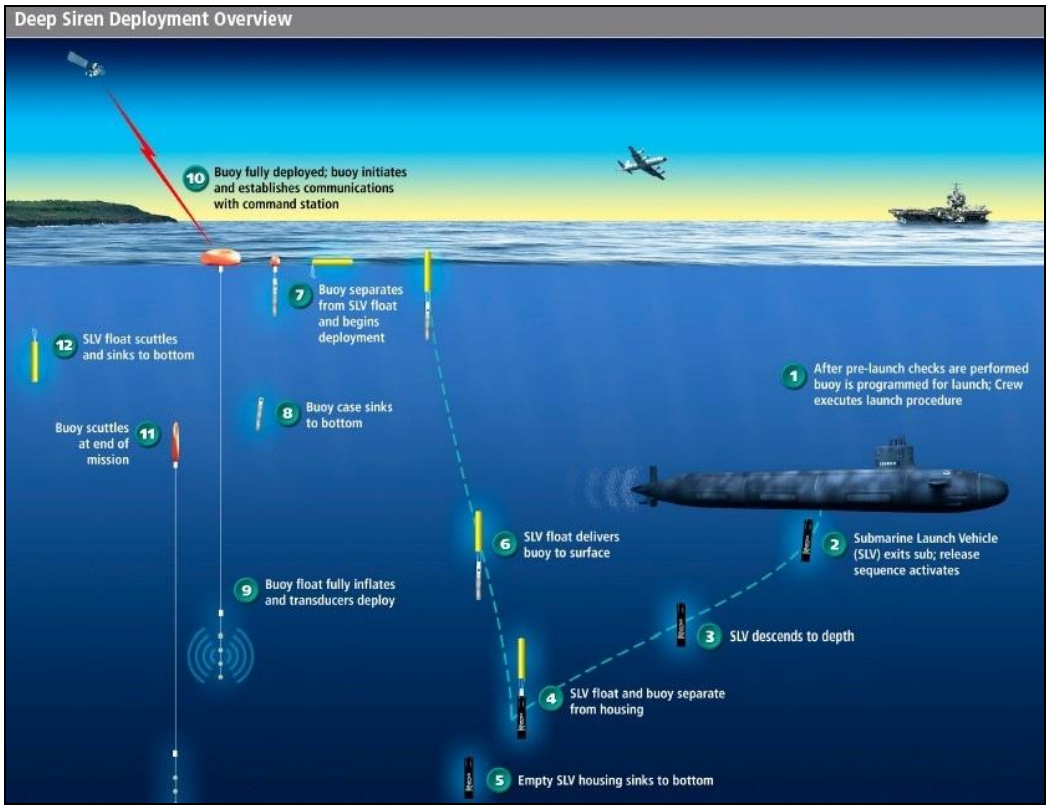

Fig 2.4 Submarine Communication

d) Hacking a Fighter Jet –

The world has 5th Generation Airplanes like F-35, F-22, J-20 , Su-57 etc and very soon we will be witnessing 6th Gen Aircraft and Unmanned Aircrafts. The above aircrafts are all digitally automated and run on supercomputers and rely heavily on communication channels like Satellites/AWACS/Radars. Therefore they are highly susceptible to hacking.

A Fighter Jet is composed of the following Digital Nodes:

- Digital Fly by wire system for flight control
- GPS, Radar & Radar warning receiver and missile warning system
- HUD & Multi-function displays
- Countermeasures dispensing system and possibly ECM pod
- Fire control computer and/or mission computer
- UHF and VHF radios and datalink
- TACAN receiver and ILS
- Secure voice and/or anti-jamming equipment
- FADEC to control engine
- TACAN, VOR/ILS, INGPS etc
- Weapon Aiming System (IR or Radar)

In the past Ethical hackers have even hacked F-15 and raised the DEFCON. Hacking a Fighter plane also means hacking the Smart Bombs which they are carrying like Spice 2000 and GBU 15.

e) Hacking an Integrated Radar Control station –

Every nation has multiple Radars placed at its borders and for tactical war planning the Radars have to be connected so that a single image of the entire enemy threat can be drawn. Since the radars are interconnected and communicate with each other hence they are susceptible to cyber attacks. Integrated Air and Missile Defense (IAMD) Battle Command System (IBCS) are the forerunner in the Radar technology and is fully automated is again prone to cyber attacks.

Usually the most regular method for infecting air gapped systems is a USB flash-drive or other removable-media. Once any air gapped system is infected, the malware can multiply to other systems on an air gapped network. Data can be retrieved the same way. The malware keeps slipped data on the system until a flash-drive is put inside, at this point the data is replicated to the drive. When the flash-drive is then inserted into another system which is connected to the internet, the data gets transmitted to the hackers command and control center.

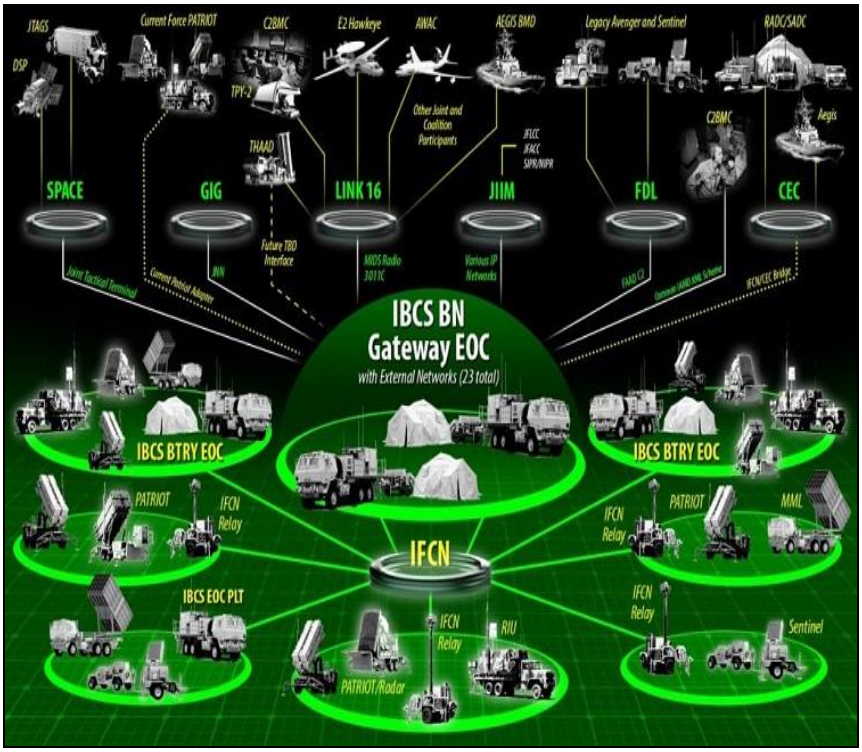

Fig 2.5 Integrated Radar Control station

3. How to protect your devices against cyber warfare

a) Use Firewalls and UTMs (Unified Threat Management)

For Companies relying on Data Center or Cloud it is necessary to Use Firewalls and UTMs. The internet should land on the UTM first then to the Router. The IP addresses should be white listed and blacklisted as per their behaviors and stored in the database, similarly only necessary ports be left open. Some important Ports which needs attention are:

SNO	Port	Vulnerabilities
1	Ports 20 and 21 (FTP)	Brute-forcing passwords Anonymous authentication (it's possible to log into the FTP port with "anonymous" as the username and password) Cross-site scripting Directory traversal attacks
2	Port 22 (SSH)	Hackers can exploit port 22 by using leaked SSH keys or brute-forcing credentials.
3	Port 23 (Telnet)	It's vulnerable to many attacks, including credential brute-forcing, spoofing and credential sniffing.
4	Port 25 (SMTP)	This TCP port is vulnerable to spoofing and spamming.
5	Port 53 (DNS)	This port is particularly vulnerable to DDoS attacks.
6	Ports 137 and 139 (NetBIOS over TCP) and 445 (SMB)	Server Message Block (SMB) uses port 445 directly and ports 137 and 139 indirectly
7	Ports 80, 443, 8080 and 8443 (HTTP and HTTPS)	They're especially vulnerable to cross-site scripting, SQL injections, cross-site request forgeries and DDoS attacks.
8	Ports 1433,1434 and 3306 (Used by Databases)	They are used to distribute malware or are directly attacked in DDoS scenarios. Quite often, attackers probe these ports to find unprotected database with exploitable default configurations
9	Port 3389 (Remote Desktop)	This port is used in conjunction with various vulnerabilities in remote desktop protocols and to probe for leaked or weak user authentication

Fig 3.1 Ports and Vulnerabilities

The organizations should have norms for **IP Whitelisting, Email Whitelisting & Application Whitelisting.**

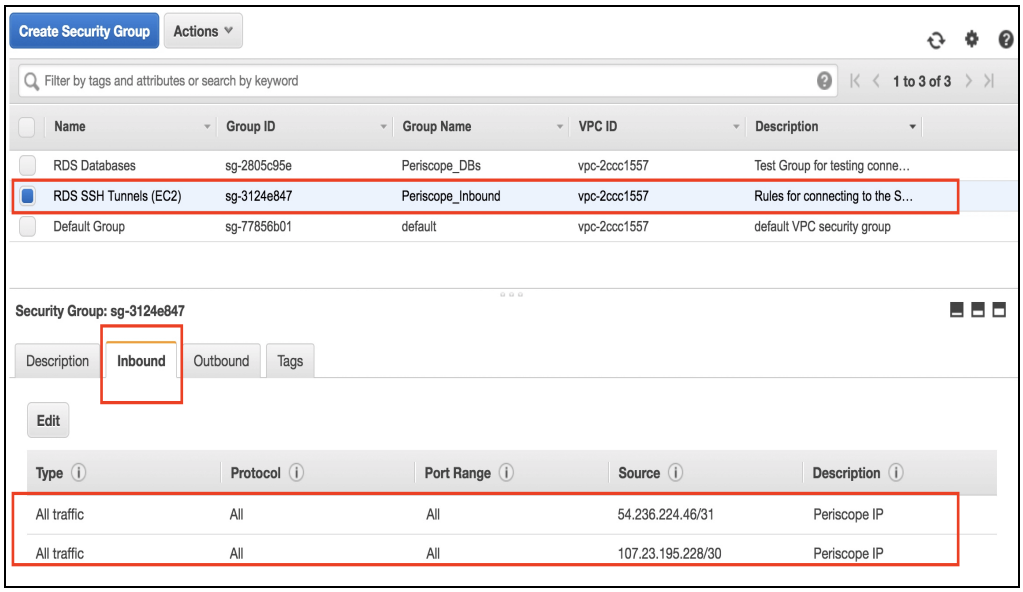

Fig 3.2 IP Whitelisting and Blacklisting

b) Use Bastion Host

A bastion-host is a devoted server that allows authorized users access a private-network from an Internet. Situated outside the firewall, the bastion-host becomes the only input path to the internal servers.

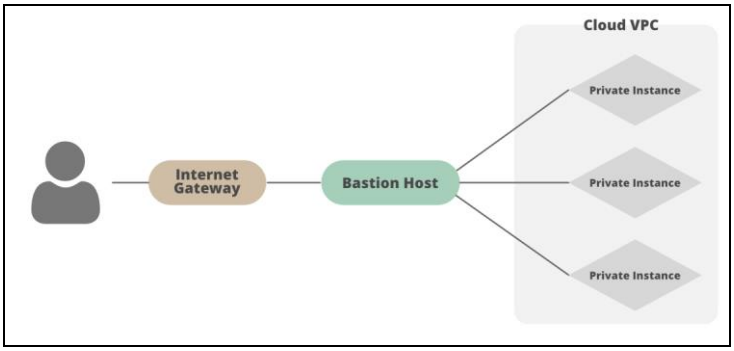

Fig 3.3 Bastion Host

c) Use DMZ for additional security

DMZs act as a buffer-zone in between the internet and the private LAN. The DMZs sub-net is placed between two fire-walls. All inbound traffic is then screened using a fire-wall before they reach at the server placed in the DMZ.

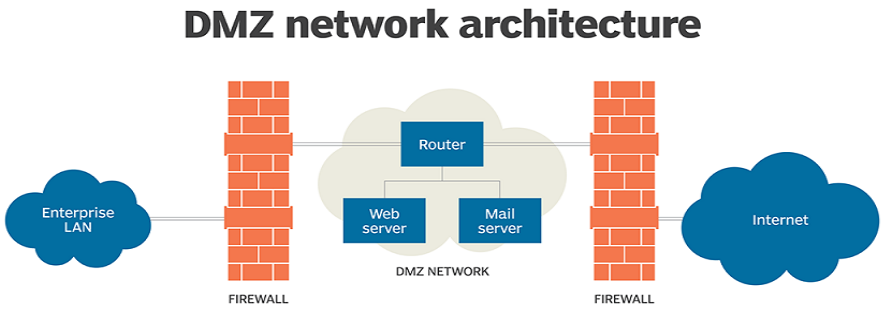

Fig 3.4 DMZ

d) Centralized Antivirus or Antivirus Collaboration

For any Enterprise it should be compulsory to have a centralized Antivirus server. The centralized Antivirus server gives the ability to monitor all the systems in the LAN and see their health and can upgrade their antivirus patches if required. This also helps in collaborating attack incidents and storing them in a central repository to be used for future incidents.

e) User Behavior Analysis using Cyber security Software

User behavior Analysis use AI & machine learning (ML) to analyze big data-sets with the aim of spotting patterns that indicate:

- Security-breaches
- Data-exfiltration
- Or other malicious activity that might otherwise go unnoticed

User behavior Analysis help enterprise assesses risks and alleviates threats before hackers can enter the networks and harm it. They also help enterprise to demonstrate compliance with industry/government regulations.

f) **Use VPN (Virtual Private Network)**

A VPN creates a secure-tunnel between a PC and the VPN-server, which conceal their online activity and position. VPN ensures to protect online privacy and foil their ISP from tracking their browsing activity.

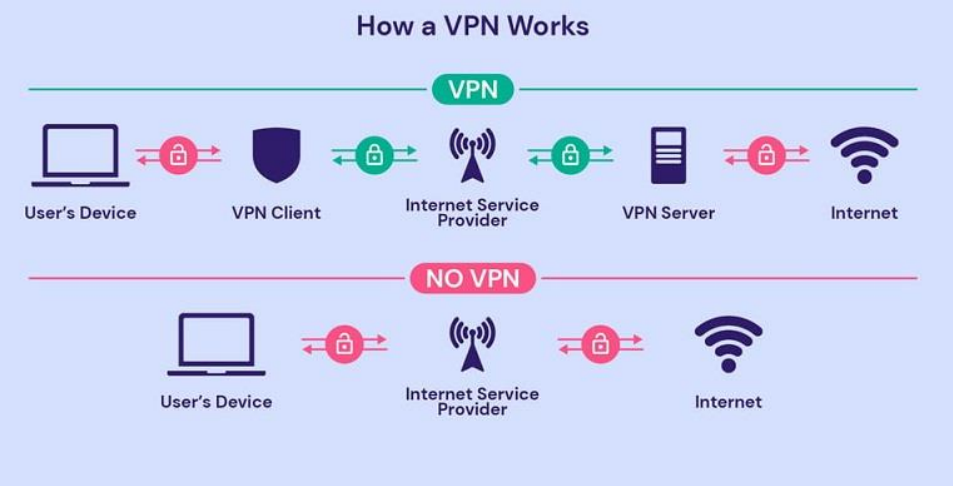

Fig 3.5 VPN

g) DDoS mitigation

DDoS mitigation is the process of shielding a targeted-server or network from a distributed denial-of-service (DDoS) attack by Detection

- Diversion
- Filtering
- Analysis

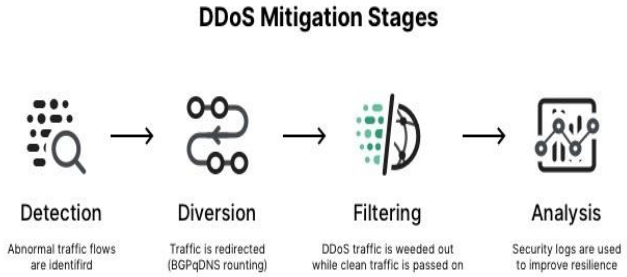

Fig 3.6 DDoS

h) Data encryption

Data encryption jumbles data before storing it in databases. This protects from unauthorized users from exploiting the data in possible data-breaches. Enterprises should use Key Management Service perform data encryption.

i) Define a Proper DC-DR Replication Policy

Even if at the most unfortunate event of any cyber attack, the DC-DR Replication policy will ensure that the data remains safe. As per the enterprise need the DC-DR can be in Active-Active or Active Passive mode. Further the RPO and RTO be defined as per the best practice policy.

j) Cyber Insurance

Cyber insurance, also known as cyber-liability-insurance, is an agreement to help mitigate the financial risks associated with online business. In exchange for a monthly/quarterly/annual fee, the insurance-policy shifts some of the risks to the insurer.

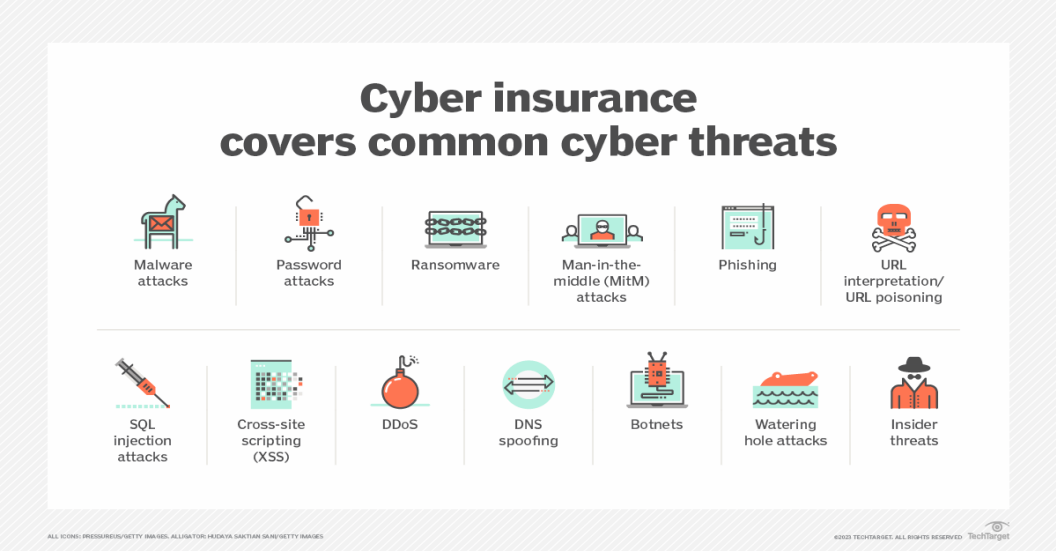

Fig 3.7 Cyber Insurance

k) Cyber Security Policy

All enterprises should necessarily have a central Cyber security policy and should strictly adhere to it. The Cyber security policy should be updated as and when required. The Cyber security policy should be drafted by keeping in mind the following actionable items:-

- Infrastructure
- Network
- Application
- Cloud
- Data Center
- Database

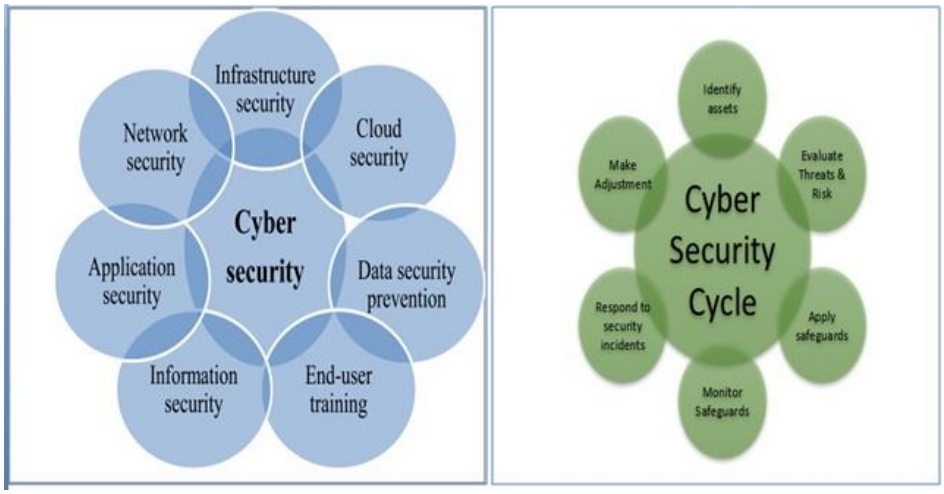

Fig 3.7 Cyber Security Policy

l) Chief Information Security Officer(CISO)

It is mandatory for all organizations to have a Chief Information Security Officer. A CISO is a senior level manager who looks after the enterprise information, cyber, and technology security. The roles and responsibilities of a Chief Information Security Officer are:-

- Implementing and overseeing your Enterpise cyber security program
- Straightening cyber security and business objectives
- Monitoring Incident-Response Activities
- Managing business-continuity and disaster-recovery
- Cyber security awareness & training

4. Some Notable agencies/Organizations in the Cyber Security Paradigm

Some Notable agencies which needs to be followed and subscribed to get the latest updates about the recent trends in cyber security.

a) CERT-In

The Indian Computer Emergency Response Team (CERT-In) is an agency under the Ministry of Electronics and Information Technology of the Government of India. It is the nodal agency to deal with cyber-security threats like hacking & phishing. It reinforces security-related defense of the Indian Internet-domain.[26][27]

CERT-IN has overlapping duties with other offices like as National Critical Information Infrastructure Protection Centre (NCIIPC) which comes under the PMO and the National Disaster Management Authority (NDMA)

b) Cyber Security Association of India

CSAI is working in close touch with Government and Industries on Cyber Security, interfacing with thought leaders, trainers, ethical-cyber experts and enhancing the cyber-safety and security to protect individual, companies, critical infrastructure and Country as a whole.

CSAI is working to establish a multi-stakeholder consortium bringing together Corporates, State/Central Governments, Academics, Defence, MNCs, PSUs, Intelligence Agencies, Enforcement Agencies and etc. to improve the state of Cyber Security both at domestic and international level. [28][29]

c) OWASP

The Open Worldwide Application Security Project (OWASP) is an online community that produces freely available articles, methodologies, documentation, tools, and technologies in the field of web application security. The OWASP provides free and open resources. It is led by a non-profit called The OWASP Foundation. [30][31]

d) ENISA

The European Union Agency for Cybersecurity (ENISA) contributes to EU cyber policy and helps prepare EU countries for future cyber challenges. [32][33]

e) Ministry of Electronics and Information Technology (MeitY)

The Ministry of Electronics and Information Technology (MEITy) is an executive agency of the Union

Government of the Republic of India. It was carved out of the Ministry of Communications and Information Technology on 19 July 2016 as a standalone ministerial agency responsible for IT policy, strategy and development of the electronics industry.

The Ministry of Electronics and Information Technology (MeitY) provides requirements and guidelines for Cloud Service Providers (CSPs) to empanel (register) their services with the Government of India. Once empaneled, CSPs are permitted to do business as per the Guidelines for Procurement of Cloud Services. [34][35]

5. Some High Profile examples of cyber warfare operations

The Russia-Ukraine crisis began in February 2022, and the war is also now happening in the cyber world. It has been observed new viper malware being used to attack Ukrainian targets and installed on at least several hundred machines across Ukraine. Several Ukrainian organizations have also succumbed to attacks that employed the KillDisk and HermeticWiper malware strands, which appear to destroy data on devices.	Iranian hackers launched a cyberattack against Israel's railroad network. The hackers used a phishing campaign to target the network's electrical infrastructure. Brazilian and UAE companies were also reportedly targeted in the same attack.	U.S. and Japanese officials warn that Chinese state-sponsored hackers placed modifying software inside routers to target government industries and companies located in both countries. The hackers use firmware implants to stay hidden and move around in their target's networks. China has denied the allegations.
Russia-linked hackers launched a DDoS attack against Vatican City servers, knocking its official website offline. The attack came three days after Russian government officials criticized Pope Francis for his comments about the war in Ukraine.	Hackers disabled digital services of the Vanuatu government in a cyberattack. The attack affected all government services, disabling emails, websites, and government systems, with only partial access restored a month later. Australian sources stated the hack was a ransomware attack.	Iranian hackers targeted Albanian computer systems, forcing Albanian officials to temporarily shut down the Total Information Management System, a service used to track individuals entering and exiting Albania. This attack closely followed Albania's decision to sever diplomatic ties with Iran as well as the American sanctions and NATO's condemnation of an Iranian cyberattack against Albania in July.
Hackers used a DDoS attack to temporarily take down the website of Taiwan's presidential office. The Taiwanese government attributed the attack to foreign hackers and stated normal operations of the website resumed after 20 minutes. Taiwan's Foreign Ministry also noted hackers targeted their website and the main portal website for Taiwan's government.	The Romanian National Directorate of Cyber Security said that multiple public and private sector websites were hit with DDoS attacks. The victims included the ministry of defense, border police, national railway company, and the OTP Bank. A group claiming credit for the attack said on Telegram that it hacked the websites because Romania supported Ukraine since the Russian invasion of the country.	The United States removed Russian malware from computer networks around the world, a move made public by Attorney General Merrick B. Garland. While it is unclear what the malware's intention was, authorities noted it could be used from anything from surveillance to destructive attacks. The malware created a botnet controlled by the Russian GRU.

* **Source – Internet and various websites**

6. Conclusion and Future Work

With the advent of technologies like Quantum Computing and Artificial Intelligence the Cyber War is inevitable The Data Center Managers the Cloud Service Providers need to be duly updated at all times to avert any Cyber Attack. The CISO of any organization will play the crucial role in this paradigm. With the introduction of digital money and crypto currencies the financial institution are highly susceptible.

Artificial Intelligence

With the arrival of A.I/Machine Learning/Deep Learning the Cyber Attacks will be increased and shall be in a more stealthily manner. AI will automate the process of creating phishing-emails using bots. Deep fake will use AI and disrupt the worlds social domain. After the use of AI it will be easier to crack a password.

Internet of Things (IoT)

With more devices getting connected to the internet, it will be of more pain to keep a watch on the cyber attacks. Because now hackers will have more endpoints to enter the system.

Quantum Computing

Quantum computing will entirely revolutionize the way we look at Cyber Crimes. The enormous power of Quantum Computing will inflict wounds deep inside and will outclass the usual computing capabilities. With quantum computing domination, every enterprise in the world that records and process data will be highly prone to a cyber attack.

7. References

1. https://www.blackhat.com/presentations/bh-dc-09/Laurie/BlackHat-DC-09-Laurie-Satellite-Hacking.pdf
2. https://theconversation.com/hackers-could-shut-down-satellites-or-turn-them-into-weapons-130932
3. https://www.reuters.com/technology/north-korean-hackers-breached-top-russian-missile-maker-2023-08-07/
4. https://www.livemint.com/news/india/top-russian-missile-makers-data-breached-by-hackers-of-north-korea-says-reportmashinostroyeniya-11691457476142.html
5. https://www.forbes.com/sites/kateoflahertyuk/2018/08/22/how-to-hack-an-aircraft/?sh=1c2e7f0c41d1
6. https://www.theguardian.com/technology/2014/jul/12/chinese-man-charged-with-hacking-into-us-fighter-jet-plans
7. https://www.popularmechanics.com/military/aviation/a25100725/f-35-vulnerability-hacked/
8. https://news.sophos.com/en-us/2017/06/29/hacking-nuclear-submarines-how-likely-is-the-nightmare-scenario/
9. https://www.theguardian.com/uk-news/2017/jun/01/uks-trident-nuclear-submarines-vulnerable-to-catastrophic-hack-cyber-attack
10. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
11. K. B. Vlahos, Special report: The cyberwar threat from north korea, Fox News, accessed 26/05/14 (February 2014).URL http://www.foxnews.com/tech/2014/02/14/ cyberwar-experts-question-north-korea-cyber-capabilities/
12. R. Wilking, Expert: Us in cyberwar arms race with china, russia, NBC News, accessed 25/05/14 (February 2013). URL http://investigations.nbcnews.com/_news/2013/02/20/ 17022378-expert-us-in-cyberwar-arms-race-with-china-russia

13. I. Traynor, Russia denounces ukraine 'terrorists' and west over yanukovich 680 ousting, BBC News, accessed 25/05/14 (February 2014).URL http://www.theguardian.com/world/2014/feb/24/russia-ukraine-west-yanukovich
14. Ukraine says donetsk 'anti-terror operation' under way, BBC News, accessed 25/05/14 (April 2014).URL http://www.bbc.com/news/world-europe-27035196
15. FBI, Terrorism definition, Online, accessed 25/05/14 (2014).URL http://www.fbi.gov/about-us/investigate/terrorism/terrorism-definition
16. Sanger, The Perfect Weapon; Healey, 'A Non-State Strategy for Saving Cyberspace'; Nye Jr, 'Deterrence and Dissuasion in Cyberspace'; Mehmetcik, 'A New Way of Conducting War: Cyberwar, Is That Real?'; Singer and Friedman, Cybersecurity and Cyberwar; Healey, 'The Spectrum of National Responsibility for Cyberattacks.'
17. Healey, 'The Spectrum of National Responsibility for Cyberattacks', 57.
18. Jon R. Lindsay, 'Stuxnet and the Limits of Cyber Warfare', Security Studies 22, no. 3 (2013): 365–404; Michael Stohl, 'Cyber Terrorism: A Clear and Present Danger, the Sum of All Fears, Breaking Point or Patriot Games?', Crime, Law and Social Change 46, no. 4–5 (2006): 223–38.
19. Bryan Bender, 'World More Dangerous, Top General Tells Harvard', BostonGlobe.com, 2012, https://www.bostonglobe.com/news/nation/2012/04/12/world-more-dangerous-top-general-tells-harvard-world-more-dangerous-top-general-tells-harvard/XrSM8cTzyZ0YstKv36JhJN/story.html.
20. Gopal Ratnam and Gopal Ratnam, 'Cybersecurity Budget up 5 Percent in 2020, White House Says', Roll Call, March 20, 2019, sec. whitehouse, https://www.rollcall.com/news/whitehouse/cybersecurity-up-5-percent-in-2020-budget-white-house-says; Sanger, The Perfect Weapon.
21. Lindsay, 'Stuxnet and the Limits of Cyber Warfare'; Alex Gibney, Zero Days, Documentary, 2016.
22. Jerry Brito and Tate Watkins, 'Loving the Cyber Bomb - The Dangers of Threat Inflation in Cybersecurity Policy', Harvard National Security Journal 3, no. 1 (2011): 39–84.
23. Thomas Rid, 'Cyber War Will Not Take Place', Journal of Strategic Studies 35, no. 1 (2012): 5–32; Jon Randall Lindsay, 'Restrained by Design: The Political Economy of Cybersecurity', Digital Policy, Regulation and Governance, 2017; Erik Gartzke, 'Making Sense of Cyberwar', Policy Brief, Belfer Center for Science and International Affairs, Harvard Kennedy School, January, 2014, 41–73.
24. Justin Joque, Deconstruction Machines: Writing in the Age of Cyberwar (University of Minnesota Press, 2018), chap. Introduction.
25. Lindsay, 'Restrained by Design: The Political Economy of Cybersecurity', 498.
26. https://www.cert-in.org.in/
27. https://en.wikipedia.org/wiki/Indian_Computer_Emergency_Response_Team
28. https://www.ncsai.in/
29. http://cmai.asia/cybersecurity/
30. https://owasp.org/
31. https://www.cloudflare.com/en-gb/learning/security/threats/owasp-top-10/
32. https://www.enisa.europa.eu/
33. https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-agency-cybersecurity-enisa_en
34. https://www.meity.gov.in/
35. https://en.wikipedia.org/wiki/Ministry_of_Electronics_and_Information_Technology

36. https://www.wired.com/2014/11/airhopper-hack/