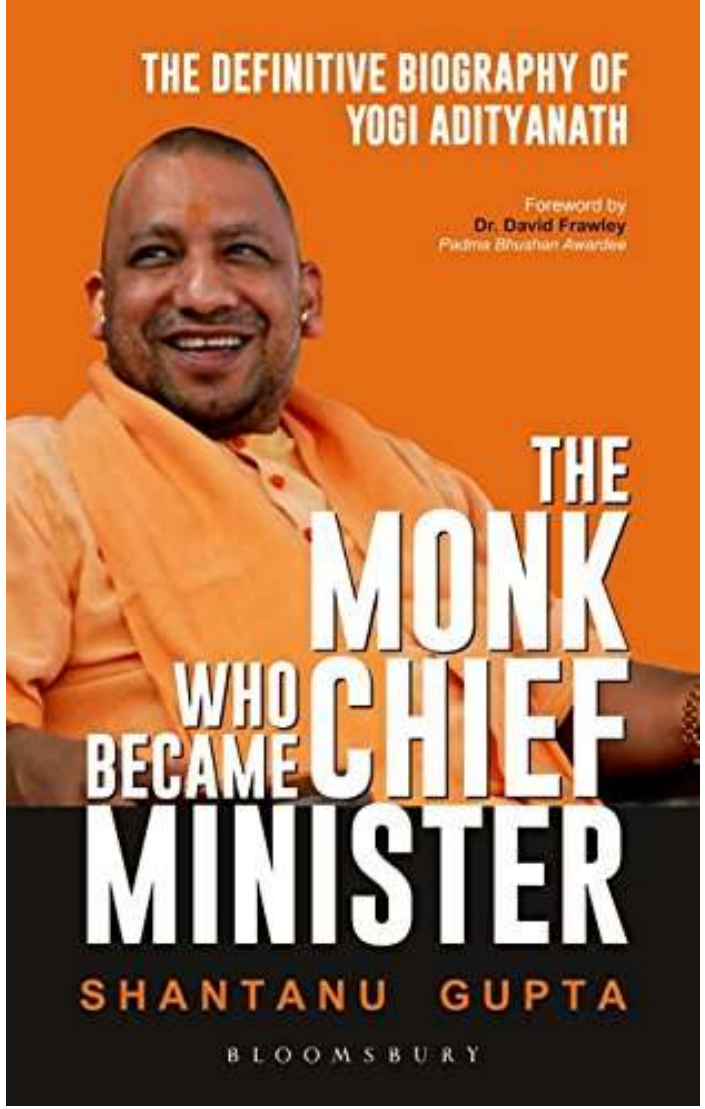
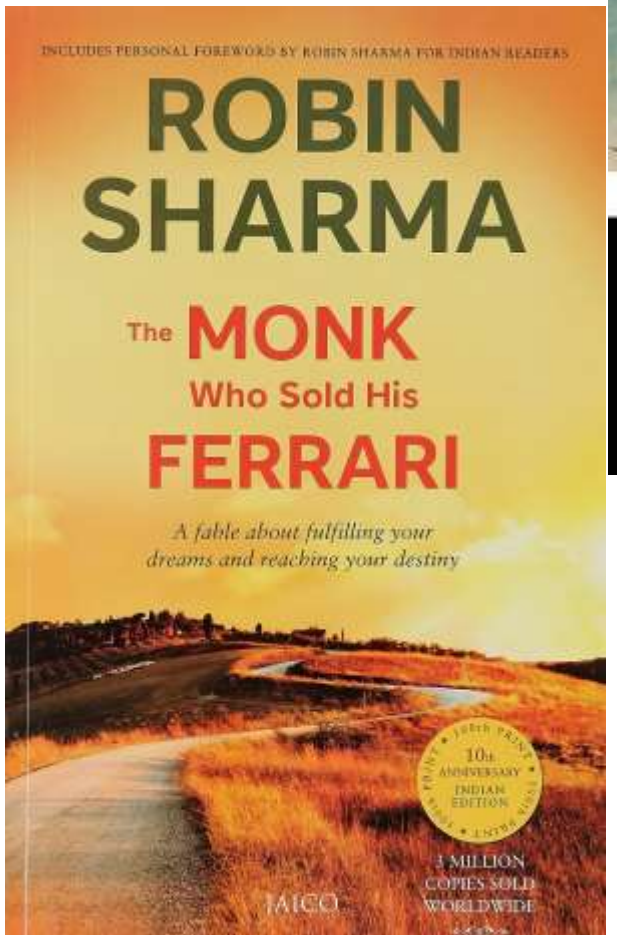
4IR and GIS : Beware of the MONK

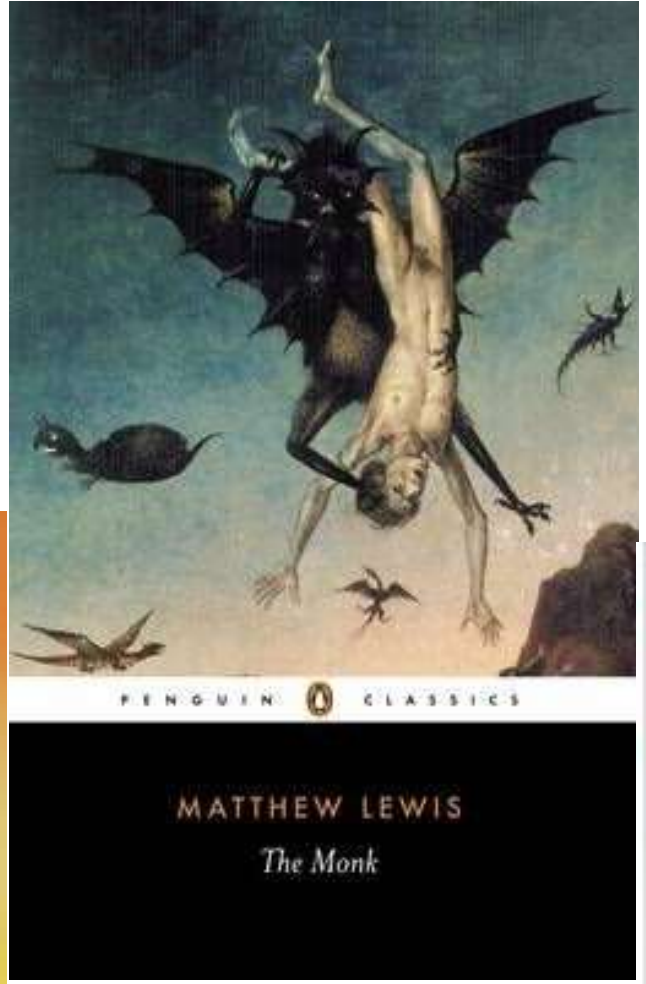
By

Lieutenant General (Dr) Rajesh Pant PVSM, AVSM, VSM (Retd)



WHAT

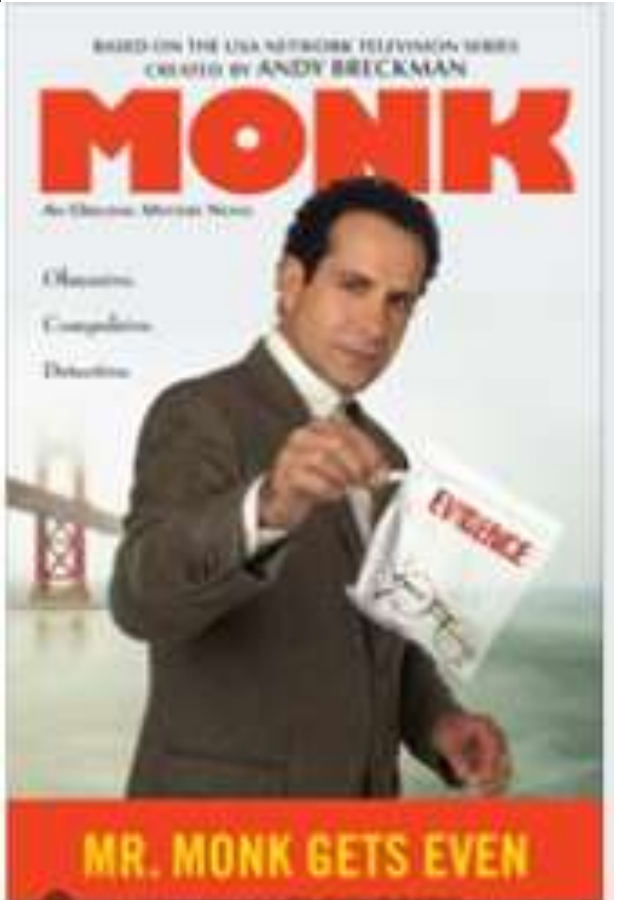




IS

THE

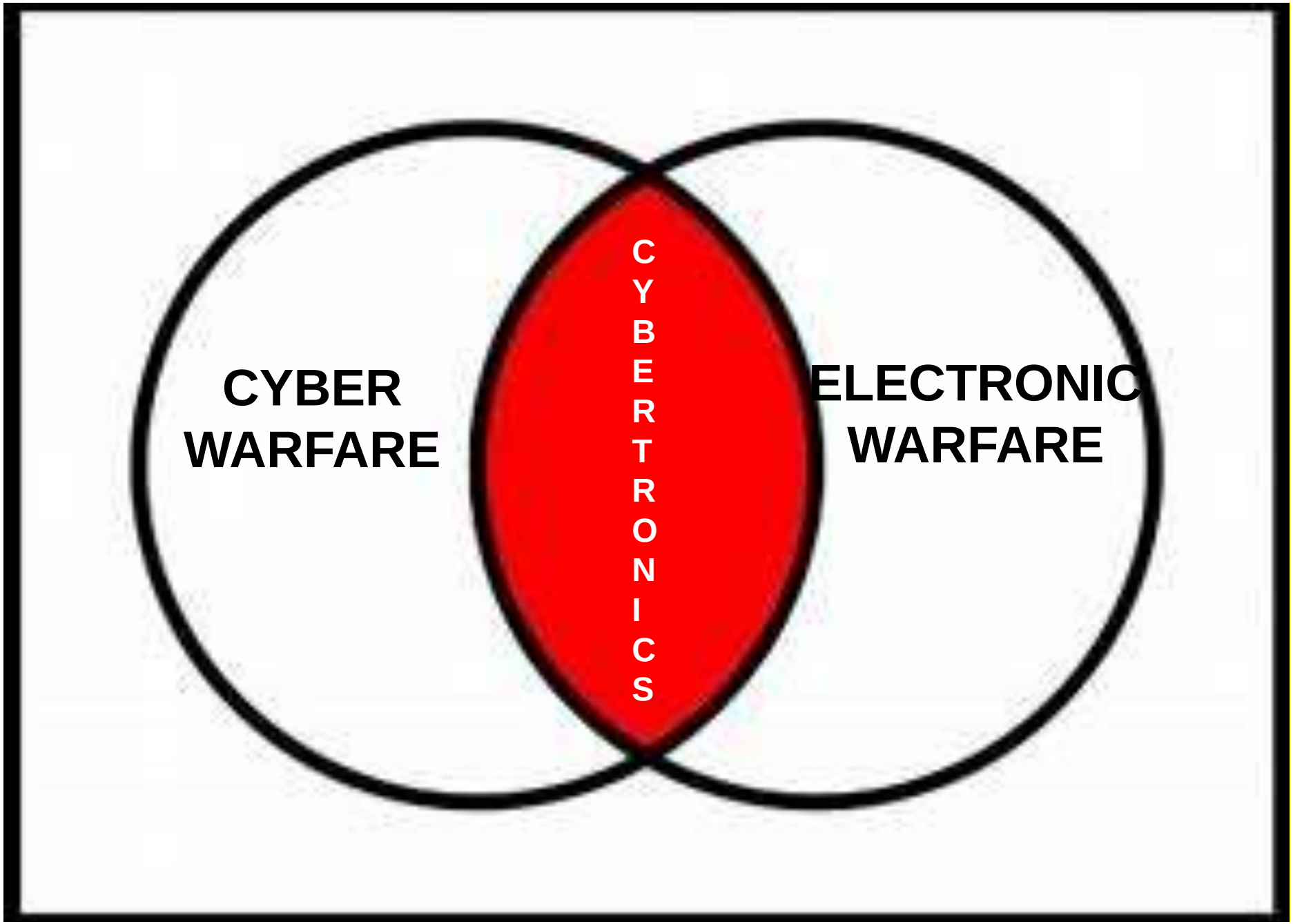
MONK ?




CYBERTRONICS
MONK= MOTHER OF NON KINETICS

What is Cybertronic Warfare ?

- ✓ The new domain of warfare is derived from the earlier two forms of **Cyber** and Elec**tronic** Warfare.
- ✓ In order to uniquely distinguish it from CW or EW, it is represented by **CeW.**
- ✓ It can be defined **as all actions involving the use of the Electromagnetic Spectrum for ingress into a networked electronics based computer system resulting in either obtaining of intelligence or soft and hard attacks against that networked system, and preventing own systems against the same.**


CYBER
WARFARE
CYBERTRONICS
ELECTRONIC
WARFARE

Key Features of CeW

- It is a non-military or military action, which can be conducted at strategic, operational or tactical levels, in coordination with the operational plans.
- It must mandatorily involve the use of both EM Spectrum and computer networks. This feature distinguishes it from the known domains of EW and CW.
- In it's passive avatar, CeW provides a source of intelligence.
- In it's active avatar, CeW can either result in insertion of malware in the computer network, perception management through the cyber domain, EM jamming of the network or even the physical destruction of the electronic components.
- It includes the preventive measures against CeW conducted by the adversary on own systems.

The Cybertronic Process

- Analysis of known information of hostile network, battlefield management systems and frequency bands of operation of wireless links in the geographical area of interest.
- Scanning of the EM spectrum in the band of interest.
- Analysis of signals, including their demodulation and demultiplexing.
- Synchronisation, deinterleaving, extraction of data or IP traffic depending on type of transmission.
- Deciding on whether to either obtain intelligence through passive means, including Direction Finding, or employment of attack vector.
- Deciding attack vector of either malware insertion or Jamming or use of Directed Energy Weapon as per operational plans.
- For malware insertion, carry out the cyber warfare stages of scan, insert, spread and execute.
- For perception management, insert the approved theme into the target cyber domain.
- For Jamming, use of EW jammer against target radar/receiver
- For Directed Energy weapon, employment of High Power Microwave Pulse from suitable platform.
- Damage assessment.
- Preventive measures against CeW by the adversary.

CeW Case Studies: OP ORCHARD

Operation Orchard was an Israeli airstrike on a suspected nuclear reactor in the Deir ez-Zor region ofSyria, which occurred just after midnight on September 6, 2007. The Israeli and U.S. governments imposed virtually total news blackouts immediately after the raid that held for seven months. Nearly four years later, in April 2011, the IAEA officially confirmed that the site was a nuclear reactor. The raid was carried out by Israeli Air Force (IAF) 69 Squadron F-15Is, F-16Is, and an ELINT aircraft. In this operation, Cybertronic Warfare was conducted as under:-

Israeli Air Force EW systems carried out electronic surveillance of the various radar systems of Syrian Air Defence (AD) systems.

The Israelis then ingressed the Syrian radars by using a Jamming signal of greater RF strength than the original reflected signal.

The radar command and control system protocols were deliberately manipulated in the cyber domain to present a false sky picture for the entire period of time that the Israeli fighter jets needed to cross Syria, bomb their target and return.

The elite Israeli Shaldag special-forces commandos had arrived at the site the day before so that they could highlight the target with laser designators, a non-kinetic weapon.

Perception management was conducted to mislead the Syrian commanders.

CeW Case Studies : Drones & UAVs

Operations On Drones and UAVs: Iran 2011, South Korea 2012, Russia 2014. On 4 December 2011, an American Lockheed Martin RQ-170 Sentinel UAV was captured by Iranian forces in northeastern Iran. The Iranian government announced that the UAV was brought down by its cyberwarfare unit which commandeered the aircraft and safely landed it.. The US government initially denied the claims but later President Obama acknowledged that the downed aircraft was a US drone and requested that Iran return it. Similarly a Scheibel S-100 Camcopter UAV crashed near Incheon on 10 May 2012. In this case the Engineers lost control of the UAV due to GPS malfunction, presumably due to GPS jammer from North Korea. In another incident on 14 March 2014, Russian armed forces were able to intercept and seize an American reconnaissance and strike UAV over Crimea. The drone, was an Israeli built MQ-5B 'Hunter', one of 18 operated by the US Army's 66th Military Intelligence Brigade.

CeW was conducted as under :-

EW surveillance was conducted to intercept the Command & Control Communication link as well as the Guidance link of the drone.

Jamming was conducted to block the Drone's command and control link communications with it's base station.

Jamming was conducted on the original GPS frequency.

GPS protocol was exploited in the Cyber domain and the guidance system manipulated to make the drone land or crash.

CeW Case Studies: Ukraine and Syria

Ukraine 2014. Ukraine was the largest battlefield of cyber war since Russia's cyber-attacks on Estonia in 2007 and Georgia in 2008. Russia hit almost all Ukraine government websites and it was able to take control and to put on surveillance and monitoring all the Internet and telephone communications lines, before the invasion and occupation of Crimea by its military. One of the techniques used by the Russians for cyber espionage was the "Snake", also known as Uroburos. It was developed in Russia in 2005 and it is capable of inducing chaos in communication system, and this is exactly what it did in Ukraine. What's interesting about it is the fact, that it is able to combine two in one. It is able to be used as a stealthy means for network surveillance and data collection, it can also carry out a 'warhead' – able to physically destroy computer networks specifically targeted by its operators.. In this case an element of the classic Anti-neck Command and Control Warfare was also employed along with EW and CW to create a classic CeW operation.

Syria 2015. In 2015, "Krasuha-4" was deployed at the Khmeimim Russian military base in Syria. During the attack by US forces on Syrian army airfield there by Tomahawk missiles, reports indicated that **"Krasuha" forced some of the missiles off-target**. The "Krasuha-4" EW system suppresses the functioning of electronics-powered stationary and mobile objects with the help of interference effects in what is described as "smart" operations in order to distinguish between enemy and friendly signals in "Krasuha'"s area of operations. **This system is capable of blinding not only enemy fighters or bombers, but also ground-based radars,** AWACS aircraft and even spy satellites, since "Krasuha"'s horizontal and vertical ranges reach three hundred kilometers. This system also counters enemy drones and unmanned systems.

Cybertronics and the F-35

Unlike legacy tactical aircraft that had "federated" electronic-warfare systems, the F-35 architecture is highly integrated. Radio-frequency and electro-optical receivers are embedded around the edge of the airframe to provide continuous sensing of hostile emitters in every direction, with collections from all sensors fused through a central computer before being displayed on the visor of the pilot's helmet. The system also merges information from off-board sensors to provide a comprehensive picture of the local electronic environment.

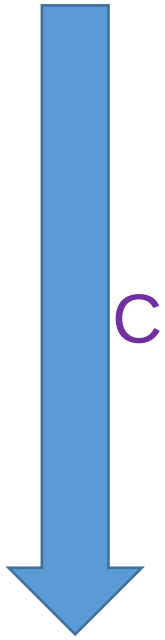
F-35 is the first fighter that integrates threat data from across the relevant segments of the spectrum before displaying it to the pilot. That reduces the time required to respond to dangers while also easing pressure on the pilot. In fact, if the pilot is preoccupied with other facets of the mission, the EW system will automatically generate the optimum solution to a threat, whether that means jamming a radar, releasing chaff to confuse it, or launching false targets (usually high-tech flares) to draw away heat-seeking missiles.

Onboard EW functions are closely coupled with the F-35's agile radar, which like many other onboard electronic systems is built by Northrop Grumman. The radar is used not only to track and target potential threats, but also to generate jamming signals that overload enemy sensor and communication receivers so that they cannot be used effectively.

Cyber Warfare Technologies

- IP Spoofing.
- Routing Attacks.
- ICMP Attack.
- Ping of Death Attack.
- Packet Sniffing.
- MAC Address Spoofing.
- ARP Attack.
- DHCP Starvation
- TCP "SYN" Attack.
- Man-in-the-Middle (MitM) Attacks
- Port Scan Attack.
- Backdoor Attacks
- Authentication Attacks.
- Phishing Attacks.
- Access Attacks..
- DNS Poisoning.
- Buffer Overflows……. Increasing list…hard attacks, ransomware

Need to understand hacking….



Scanning.

Entry.

Lateral spread.

Control of victim device.

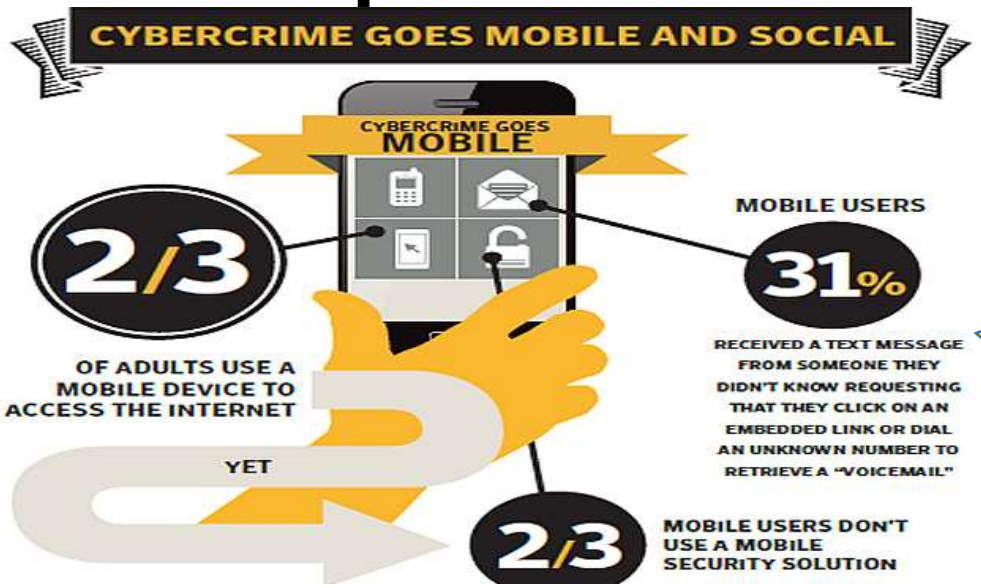
Exploitation.

Exfiltration.

Exploits, Attack Vectors , Zero Day attacks.

Ransomware, reputation holding back reporting of Cyber crimes

Mobile phone vulnerabilities…



PM says no mobiles in Cabinet meetings !

1. Android…most popular ! IOS also affected.
2. Generally malware injected through third party apps.
3. Roots the device…..gains privileged control.
4. Steals user data, can install backdoors.
5. Off-the-air interception.
6. Apple, Blackberry privacy issues.

Electronic Warfare Technologies

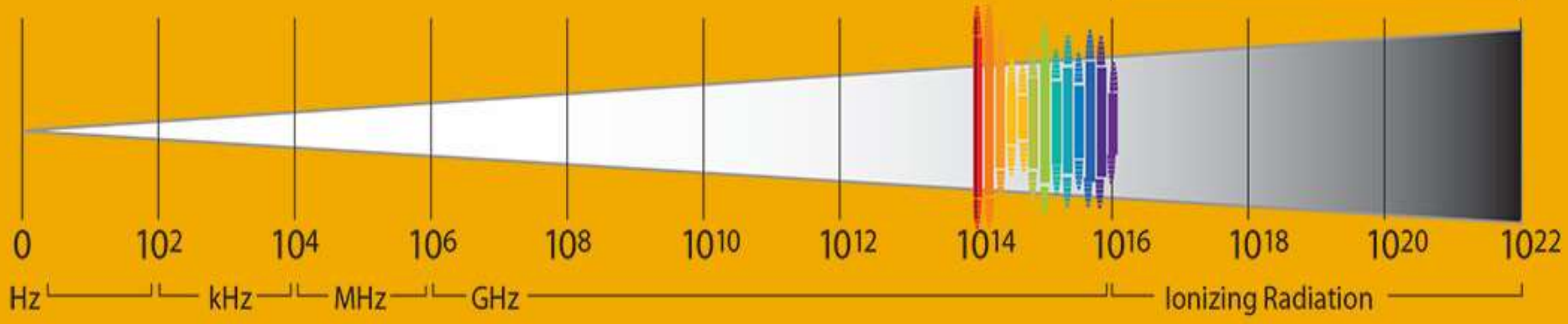
- EM Spectrum scanning
- Search, Interception and Monitoring
- Direction Finding
- Demodulation and Demultiplexing
- Extraction of data stream or packets
- Jamming
- Manipulative Jamming
- Directed Energy Weapons

Krasukha EW System

Electromagnetic Spectrum

Frequency in Hertz (Hz) or cycles per second

High energy photons on this end of the scale can break chemical bonds and damage cells



0 10^2 10^4 10^6 10^8 10^{10} 10^{12} 10^{14} 10^{16} 10^{18} 10^{20} 10^{22}

Hz — kHz — MHz — GHz — Ionizing Radiation

Direct current

Extremely low frequency

Computer

AM radio

VHF 2-6
FM radio
VHF 7-13
UHF

Radar

Microwaves

Far infrared

Thermal infrared

Infrared

Near infrared

Infrared radiation

Visible light

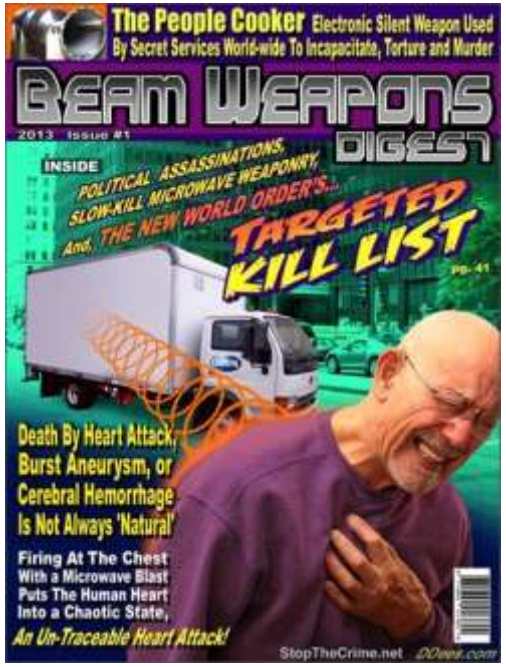
Ultraviolet radiation

X-rays

Gamma rays

Electromagnetic Weapon Systems

- New targets…Power Grids, Civil Telecom Sys, Tpt, Financial Sys, Mass Media…
- Underground Comd & Control sys also affected (Front/Backdoor coupling)
- Target LAN, SMPS, LNA, PCs, CMOS components
- Permanent damage at 2KV/m. even if eqpt is off. More eff at 1 – 3 GHz
- Ground based AD sys (defensive), or air delivered (Offensive) sys
- 10 GW power required to generate fd str of 1 KV/m at 1 Km.
- Chemical energy used in air explosion to generate electrical energy & EMP



Mobile LASER weapon

This Mobile High-Energy Laser-equipped Stryker was evaluated April 12, during the 2017 Maneuver Fires Integrated Experiment at Fort Sill, Oklahoma. The MEHEL can shoot a drone out of the sky using a 5kW laser. (US Army photo)

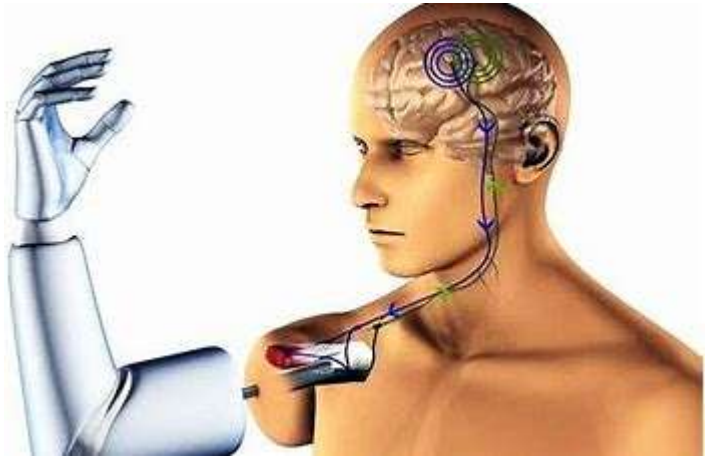
Industry 4.0 & AI: An easy Ambush Site

Industry 4.0 is a name for the current trend of automation and data exchange in manufacturing technologies. It includes cyber-physical systems, the Internet of things, cloud computing and cognitive computing.

Industry 4.0 creates what has been called a "smart factory".
Some examples for Industry 4.0 are machines which can predict failures and trigger maintenance processes autonomously or self-organized logistics which react to unexpected changes in production.

The Achilles Heel of Industry 4.0 therefore includes the software applications, hardware electronic components and the wireless networks. This is the target of Cybertronic Warfare, which is the convergence of Cyber and Electronic Warfare.

CES 2018
Brain Robotics- AI Powered Robotic hand



eCar by Toyota

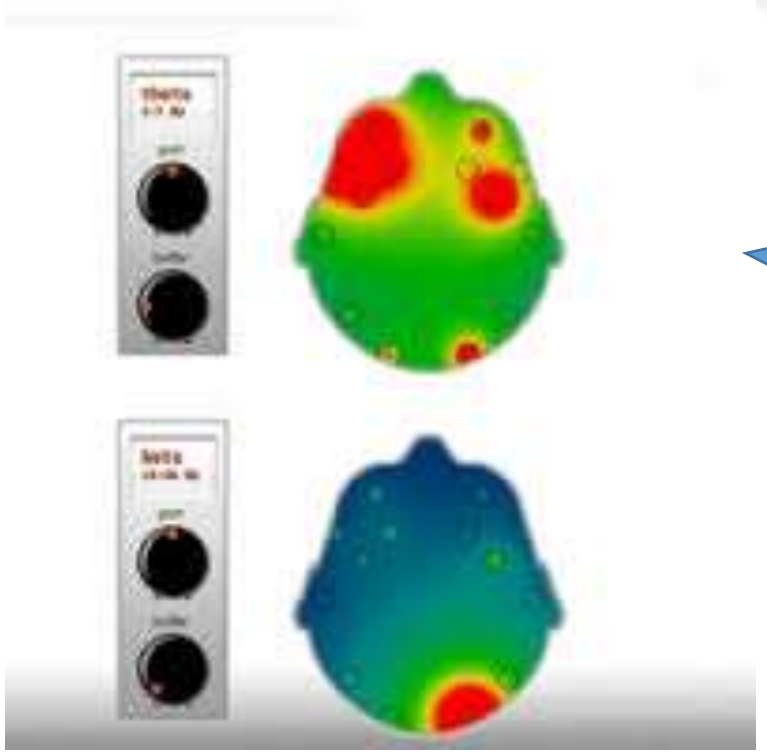
Medical Sensing with Mobile Apps

AIBO Robot of Sony

AI enabled Cyber Attacks

emotivo
you think, therefore, you can

LiFi…200 Gbps
Nano satIs
Micro UAVs



5G@60 GHz..
Human Era

Innovation Age…
Imagination

Cybertronic Domain…

Your Home

You

Your Life !!!

Driverless cars, aircraft, smart weapons…

Your laptop Or mobile	⟷	Your WiFi Router	⟷	Cable Or Radio	⟷	Internet Service Provider	⟷	Global Router Network	⟷	Data Centre Servers

Finally, my compliments to Geospatial Media team for spreading the importance of Defence and Security and its impact on Industry 4.0.

"The Society that separates its scholars from its warriors will have its thinking done by cowards and its fighting done by fools"

General Sir WF Butler

Afghanistan, 1889

CeW

Thanks…