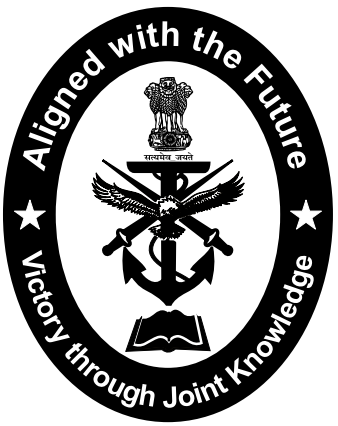
DEFENDING/ EXPLOITING EM SPECTRUM AGAINST/FOR CYBER WARFARE

Defending/Exploiting EM Spectrum Against/For Cyber Warfare

By

Brigadier Saurabh Tewari



Centre for Joint Warfare Studies
Kashmir House, Rajaji Marg, New Delhi-110 001
Tel. Nos: 011-23792446, 23006535, 23006538/9, **Fax:** 011-23792444
Website: http://cenjows.gov.in, **e-mail:** cenjows@cenjows.gov.in

Price in India : ₹150 /-

Printed in India

Printed by
Xtreme Office Aids Pvt. Ltd.
Basement Bhanot Building (Below Syndicate Bank)
Nangal Raya Commercial Complex, N.D-110046
Ph.: +91-9811707220
E-mail: xtremeofficeaids@gmail.com
Website: www.xtremeonline.in

Defending/Exploiting EM Spectrum Against/For Cyber Warfare

Disclaimer

The views expressed and suggestions made in this work are solely of the author in his personal capacity and do not have any official endorsement. Attributability of the contents lies purely with the author.

Abstract

Till about early 90s,there were two clear cut communication domains: one of telecom, and the other of computers- one for voice and other for video/data communications. However, as technology progressed we saw telecom products being developed on computer platforms, services migrating from hardware centric to software centric approach. Multiple applications converged into singular devices, and the boundary lines between telecom and IT (Information Technology) started blurring. Mobile technology, in particular smartphones and tablets, has integrated a number of technologies, and the ability to transmit wirelessly. The mobile-phone infrastructure is different from traditional fixed-line networks where the data and voice channels are separate. With mobile phones, it is feasible that data-based attacks can impact the voice channels. The introduction of voice over IP (VoIP) protocol allows voice to be carried over the data networks. These forms of communication are susceptible to standard network attacks. Examples may include disruption by Denial of Service (DoS) and possible eavesdropping of communication. Mobile phone being a wireless device by definition (and being the gateway to internet), is therefore susceptible to exploitation of the EMS (Electro Magnetic spectrum). Satellites systems are controlled by computers, which may further be connected to the military cloud or an air-gapped network in the Tactical Battle Area (TBA). The interception/jamming/DoS of satellite signal is easier compared to terrestrial

wireless systems. Cyber attacks on satellites have been reported in the past, wherein the telemetry signal was tampered to cause malfunction. To sum up, the network technology is moving towards IP for all services, and connectivity is becoming more and more wireless. So, while the cyber warfare gateway has traditionally been at layer 3 (IP Layer) and above, the means to access &infect a computer network are now available at physical layer in the form of Radio Frequency (RF) linkages. The situation gets further complex by the entry of concepts like Internet of Things (IoT). Traditional EW tools can be used to create mayhem to this ubiquitous network of things, by simple RF level brute force jamming. Military networks are no exception to technology, and are following suit. Technologies like mobile phone, satellites, wireless backhaul radios, software defined radio (SDR)etc are proliferating in military networks galore. Apropos, they are vulnerable to cyber attacks through wireless channels.

This paper explores the possibilities of conducting cyber warfare through exploitation of the EMS, with specific reference to military ICT networks in the Tactical Battle Area (TBA). It also suggests means to protect own ICT networks against adversaries.

INTRODUCTION

General

1. It is well stated that military revolution occurs with the application of new technologies combined with innovative operational concepts and organizational adaptation in a way that fundamentally alters the character and conduct of conflict. It does so by producing a dramatic increase- often an order of magnitude or greater- in the combat potential and military effectiveness of armed forces.

2. Information and Communication technologies (ICT) can fundamentally change the way military operations are conducted. By being able to integrate operations more effectively, overwhelming degree of simultaneity can be achieved. The Gulf war provided a vision of a potential revolution in which Information Age technology combined with appropriate doctrine and training, was used with unprecedented efficiency. Rapidly gaining and exploiting information

dominance was clearly a key goal of the Desert Storm campaign. The first Iraqi targets attacked were air defense, leadership (including Command, Control, Communications, and Intelligence- C3I), and electrical grids, all of which had the highest priority because of their impact on the Iraqis' flow of information. The wars in Iraq and Afghanistan also challenged operational commanders with new and emerging cyberspace and Electromagnetic Spectrum (EMS) threats. Insurgent forces, for instance, commonly operated within cyberspace by using the Internet to promulgate their messages, while at the same time, insurgents physically threatened soldiers by employing weapons enabled by the EMS, such as command and control of direct/ indirect fires and Radio Controlled Improvised Explosive Devices (RCIEDs).

3. The potency and overwhelming lethal effects of cyber warfare has outpaced the technological development in conventional military weapons space, changing the very character of future wars, and the role of cyber warfare in them. Worldwide cyber warfare is now being acknowledged as the 5th dimension of warfare (after Land, Air, Sea and Space).

Technology Scenario: The Blurring Lines Between Telecom and IT

4. In the good olden days we had a transistor radio, camera, calculators, television, landline phone, fax and computers as separate devices to access different applications like audio broadcast, photography, mathematical calculations, video broadcast, voice communication, document exchange, and data/mail exchange respectively. There were twoclear cut domains: one of telecom, and the other of computers/IT. However, as technology progressed we saw telecom products being developed on computer platforms, services migrating from hardware centric to software centric approach. Services started getting delivered as an application over a (big or small) common computing platform. Multiple applications converged into singular devices, and the boundary lines between telecom and IT started blurring. Today we have smartphones that are capable of providing voice, data, video services, and in addition provide functions like camera, radio, calculator, scanner, web browser, internet hot spot and so on. Proliferation of mobile internet to remote parts of the country gave a further boost to smartphone proliferation and usage. Mobile phone being a wireless

device by definition (and being the gateway to internet), is therefore susceptible to exploitation of the EMS, to carry out traditional EW functions, or more devastatingly, the cyber warfare. Backbone networks are a good mix of terrestrial and wireless radio links; in the last mile devices are connecting through Wi-Fi, Bluetooth and other such short haul technologies. Further, if we see the profile of telecom equipment, they are mostly being provided as a software service over a computing platform, whether it is a router, a switch, an IP radio, and so on. Even the traditional TDM services like voice are now being provided over computer networks as an IP service (VoIP- Voice over IP).If that was not enough, traditional telecom hardware based systems like satellite andDWDMsetcare being managed through computer systems, which are vulnerable to cyber warfare, including through exploitation of EMS via a wireless backbone IP radio link, or a wireless access point. This convergence has also given rise to the commonly used term ICT. To sum up, the network technology is moving towards IP for all services as well as network management, and connectivity is becoming more and more wireless- in backbone and in access.So, while the cyber warfare gateway has traditionally been at layer 3 (IP Layer) and above (in OSI model), the means to access/infect a computer network are now also available at physical layer in the form of RF linkages.The situation gets further complex by the entry of concepts like Internet of Things (IoT);mobility demands wireless connectivity, and if IoT is to succeed, it has be wireless. This opens up the Pandora'sbox insofar as the vulnerability to cyber warfare is concerned.

5. **<u>Military Networks</u>**. In military networks also we see this wave of change. The traditional CNR is now migrating to SDR which (being a computer basedplatform) gives opportunity to carry out cyber warfare through exploitation of RF spectrum.Satellite phones, cellular phones, and trunked radio systems are also being used by the modern soldier in battle field.The tactical command and control, logistics and traffic clearance networks (voice/data/video) are also transiting to IP based MANETs (Mobile Adhoc NETworks), with short haul IP radio wireless links in the backbone. Further, as concepts like the IoT become a reality in the networked battle field, the vulnerability of networks to exploitation through the EMS will increase manifold.This changed battle field communication and IT environment gives both sides enough opportunity to

exploit EMS for conduct of CNE (Computer Network Exploitation) and CNA (Computer Network Attack).This breaks another traditional rule: cyber warfare which was historically associated at strategic level (in state level conflicts)is now available at tactical and operational levels also, albeit limited in its effect to probably the battle field networks, and not impacting the national level critical information infrastructure.

6. **Convergence**. As discussed above, the proliferation of wireless technologies has moved cyber operations into the EMS which was traditionally dominated in the military context by Electronic Warfare (EW). Similarly, platforms for conduct of EW operations are migrating from discrete electronic platforms to computing platforms. Apropos, EW and cyberspace operations are becoming increasingly more intertwined, and have potential for synergistic effects. The ability to leverage both EW and Cyber Warfare capabilities as an converged system, acting as a 'force multiplier' will improve the commanders' ability to achieve desired offensive and defensive overmatch in the battlefield.In many regards cyberspace and the EMS also defy geographic boundaries, which means units can impact outside of their area of operations, and can be impacted by actors outside their area of operations. Given the commons principle above, Cyber/Electro-Magnetic (C/EM) activities must be understood as inherently joint activities. In a conventional war, military commanders always experience a gap between the Area of Interest and the Area of Influence; with a converged approach, the Area of Influence that can be achieved by a military commander is endless.

EW/Cyber in Recent Global Wars

7. The Gulf War demonstrated the central importance of EW to the conduct of a modern air war. So overwhelming was the weight of the initial attack, that the Iraqi Integrated Air Defence System collapsed in hours, never to recover to even a semblance of functionality.[1]

8. Operation Orchard (Sep 6, 2007) was probably the first demonstration of a converged EW and cyber effort in modern warfare. The operation comprised of an Israeli airstrike on a suspected nuclear reactor in the DeirezZor region of

Syria, which occurred just after midnight. The attack pioneered the use of the Israel's cyber & EW capabilities, as Israel Air Force systems took over Syria's air defense systems, feeding them a false sky-picture for the entire period of time that the Israeli fighter jets needed to cross Syria, bomb their target and return.[2,3] The technology used by Israel is said to be supported by the US Senior Suter program (developed under the Big Safari unit of US Air Force).[4] It is widely speculated that Digital Radio Frequency Memory[5] (DRFM) technology was used to feed misleading information to the Syrian air defence radar system.[6]

9. Similarly, the Russia-Ukraine conflict in 2014 adequately demonstrated the converged operations effect of Information Warfare (IW) tools.

COMMONALITIES BETWEEN EW AND CYBER WARFARE

10. Revolution in ICT is not only an important military but also a political and strategic tool for global and regional security policies of the future. But for real change to occur, it is not only the technological edge which is mandatory, but also the transformation in military culture, organization, strategy, tactics, training, equipping and logistics. Thus, ICT has led to IW being developed as a tool of modern welfare. Thefocus and notion of victory would change from destruction based concept of war to a paralysis based model.

11. Information Warfare can be said to comprise of the triad of **"PEOPLE, PROCESS AND TECHNOLOGY"**. The same is true for EW, cyber warfare or even psychological warfare.

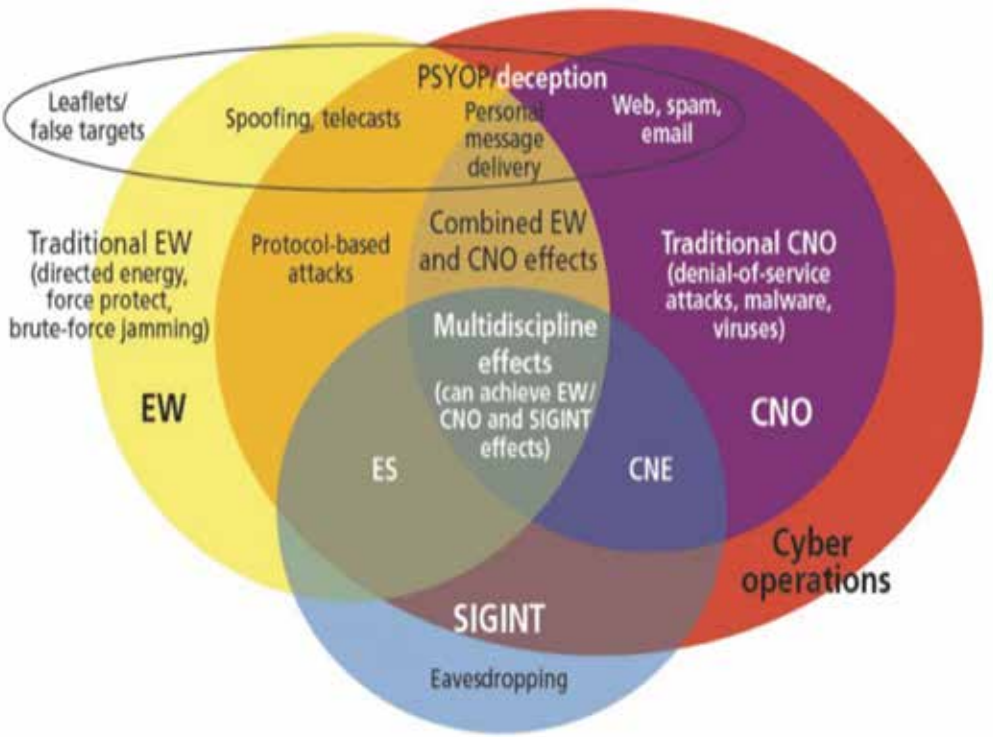
12. In this triad there are overwhelming similarities between EW and Cyber Warfare.

(a) People. The set of people who plan and execute EW operations and cyber operations are ICT engineers. Without the base domain knowledge of ICT, conduct of operations in these domains is well nigh impossible.

(b) Process. There is a one-on-one correlation between the various EW and Cyber Warfare functions. The same is given in table below:-

Operational Function	**EW**	**Cyber Warfare**
Collect information about enemy.	**Electronic Support (ES)** Listen to enemy EM transmissions to determine his capability and Electronic Order of Battle. Primarily Intelligence gathering tool.	**Computer Network Exploitation (CNE)** Spyware – Information/ activities of host PC sent to attackers location. Primarily Intelligence gathering tool.
Interfere with enemy's operational capability.	**Electronic Attack (EA)** Either interferes with the received information (jamming) or gives inaccurate outputs (deception).	**Computer Network Attack (CNA)** Viruses/ Trojans, wormsetc - which reduce available computing resources or modify programs to prevent proper processing of outputs.
Protect friendly capability from enemy's Interference	**Electronic Protection (EP)** Prevents enemy from jamming and intercepting own electronic transmissions.	**Computer Network Defence (CND)** Passwords and firewalls, security policies, anti-virus suites, which prevent malwares from penetrating & attacking a computer network.

Cause enemy systems/ people to take wrong decisions.	**Deception** Decoys depict actual targets and deceive the enemy.	**Deception** Malwares enter enemy computer network in the disguise of legitimate software and deceive the system by sending false messages.



Functional View of Converging Areas (CNO-Computer Network Operations- shown in the figure above are basically offensive cyber space operations i.e. CNE and CNA)

Source: SenftMaj Michael, Jan 4 2016, *Convergence of Cyberspace Operations and Electronic Warfare Effects*, Cyber Defence Review (https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1136055/convergence-of-cyberspace-operations-and-electronic-warfare-effects/) Accessed 28 Aug 2018

(c) **Technology**. EW and cyberspace operations are complementary and have potential synergistic effects. For example, use of an airborne weapons system to deliver malicious code into cyberspace via a wireless connection would be characterized as "EW-delivered computer network attack". The expanded use of wireless networking, digital computing and communication, along with the integration of computers with Radio Frequency (RF) communications equipment contribute to its significance in Information Operations (IO) activities. This blurs the distinction between EW and Cyber Network Operations (CNO) significantly. It is a fact that the more integrated EW and CNO are, the easier the intelligence collection, manipulation, and dissemination of information. Dependence on the EM spectrum as a medium to exchange information between computers brings in the possibility of electronic intrusion into a computer through EMS. It is thus crucial to take into account EW aspects during the conduct of CNE, CNA and CND. Electronic Protection (EP) is as important as CND,as friendly computer networks must now be protected from both Electronic Attack (EA) and CNA. Similarly, EW weapons platforms are no longer discrete electronic based systems. These are now being developed on computer platforms, be it a Software Defined Radio (SDR), or microcontroller based jammers and DF systems. Apropos, the dividing lines between EW (which targeted enemy communication systems- through EMS) and the Cyber Warfare (which targeted enemy computer networks) are blurring.

ENVIRONMENT SCAN

Indian Defence Forces

13. Without a doubt future wars are likely to be characterized by ascendancy of technology. In this regards, the documents ***"INFORMATION WARFARE DOCTRINE FOR THE INDIAN ARMY:*** 2010" published by Headquarters Army Training Command (ARTRAC), and ***"JOINT DOCTRINE FOR ELECTRONIC WARFARE : 2010"*** published by Headquarters Integrated Defence Staff (IDS), Ministry of Defence (MoD) are two major documents which lay down the doctrinal concepts in Information Warfare (IW)/EW domains.

These documents do recognise the overwhelming advances in improved communication, information, surveillance, reconnaissance capabilities and networked command and control elements, which must be gainfully exploited to fight a high-tech warfare, but do not consider any serious convergence between EMS and the cyber warfare.

US Defence Forces

14. The US Army and Navy have already recognized the need for Cyberspace-EMS alignment and moved forward in organizationally aligning their services' cyberspace and EMS operations. Both services also published roadmaps/assessments, the Army in the ***"Army Cyber-Electromagnetic Contest Capabilities Based Assessment",***[7] and the Navy in the ***"U.S. Navy Information Dominance Roadmap 2013-2028".***[8] These publications highlight a future information environment dependent on the EMS and convergence of cyberspace and EMS capabilities.

15. The US Army has disbanded its EW division, and incorporated the EW division into a newly established Cyber Command at the Pentagon.[9] Under the Integrated Cyber and Electronic Warfare program (ICE), the U.S. Army's Communications-Electronics Research, Development and Engineering Center (CERDEC) is working to identify ways to combine EW capabilities with cyber warfare tactics and enable rapid deployment of new and improved capabilities.[10] The US Army official website states:[11]

> *"United States Army Cyber Command and Second Army directs and conducts integrated electronic warfare, information and cyberspace operations as authorized, or directed, to ensure freedom of action in and through cyberspace and the information environment, and to deny the same to our adversaries."*

16. As late as Apr 2017, the US Army has come out with a new Field Manual, the FM 3-12 (which supersedes the earlier FM 3-38) titled "Cyberspace and Electronic Warfare Operations".[12] The new manual emphasizes the need to carry out integrated CEMA (Cyber Electro Magnetic Activities) operations in all phases of war; it says:

In the future, as adversary and enemy capabilities grow, our ability to dominate cyberspace and the EMS will become more complex and critical to mission success. Incorporating Cyberspace Electromagnetic Activities (CEMA) throughout all phases of an operation is key to obtaining and maintaining freedom of maneuver in cyberspace and the EMS while denying the same to enemies and adversaries. CEMA synchronizes capabilities across domains and war fighting functions and maximizes complementary effects in and through cyberspace and the EMS.

17. The US Navy has a concept of Electromagnetic Manoeuvre Warfare, which also aims to integrate cyber, jamming, spoofing, and careful manipulation of electronic signals to blind and baffle enemies.

18. The US AF did a study in Feb 2014[13] wherein it clearly brings out its shortcoming:

What the US Air Force has not done well to date is align its efforts in cyberspace operations with its electronic warfare and EMS operations missions in a way that effectively and holistically leverages the EMS and cyberspace to their greatest potential. The Army and Navy already recognized the need for cyberspace-EMS alignment and moved forward in organizationally aligning their services' cyberspace and EMS operations.

Chinese PLA

19. The Chinese have adopted a formal IW strategy called "Integrated Network Electronic Warfare" (INEW) that consolidates the offensive mission for both CNA and EW, under 4th Department (Electronic Countermeasures) of PLA General Staff Department (GSD). PLA theorists have coined the term "Integrated Network Electronic Warfare" to outline the integrated use of EW, CNO, and limited kinetic strikes against key command and control, communication and computers nodes to disrupt the enemy's battlefield network information systems.[14]

20. The PLA sees cyber warfare as a first-strike option to preclude the requirement of conventional military operations, and not as a force multiplier

to conventional operations.[15] China has created a new force called the Strategic Support Force (SSF) in 2015, which will form the core of China's information warfare strategy, and is likely to integrate reconnaissance, early warning, cyber, communications, command, control, navigation, digitalized ocean, digitalized land, etc. and will provide strong support for joint operations for each military service branch.[16,17,18] In addition, the space assets are also put under the SSF. The SSF is being touted as the 5th Service and not just another military branch of the PLA.

21. Exploitation of EMS for cyber warfare is very much part of the Chinese strategy, as a research paper by John Costello, titled "Chinese Views on the Information "Centreof Gravity": Space, Cyber and Electronic Warfare" published by the Jamestown Foundation, states:[19]

With physical or network access limited by geopolitical borders, Internet embargos and increased cyber security under threat or reality of cyber-attack, the most promising avenue, then, is via the electromagnetic spectrum (for example, wireless radio) that connects these machines. In war-time, the Internet is no longer an option for cyber-attack. Information operations planners have to plan for a contingency where the electromagnetic spectrum is the only viable option.

Cyber warfare, limited in a war-time environment by "Internet embargos," can still be heavilyutilized over the electromagnetic spectrum. Effecting a network "invasion" via injection of malware over the electromagnetic spectrum is apriority, despite serious technological barriers.

Russian Defence Forces

22. According to Maj-Gen Stephen Fogarty, head of the U.S. Army's Cyber Center of Excellence :[20,21]

"Russian activities in Ukraine (in 2014)... really are a case study in the potential for CEMA, Cyber-ElectroMagnetic Activities… It's not just cyber, it's not just electronic warfare, it's not just intelligence, but it's really effective integration of all these capabilities with kinetic measures to actually create the effect that their commanders want to achieve."

23. When the Russians went into Ukraine, they basically shut down all the military systems, and the Ukrainian soldiers used their cell-phones, and they got located and destroyed. This Russian-style integration of cyber/EW, drones, and old-fashioned high explosive is a fair glimpse of the future wars.

24. As per a statement of Russia's Defence Minister Mr Sergei Shoigu in the parliament in 2016, Russia plans to form a new branch of its armed forces to focus on information warfare.[22]

Australian Defence Forces (ADF)

25. The Australian Defence Force Cyber and EW Division (CEWD) undertakes *"research and development focused on identifying, analysing and countering threats to Australia's defence and national security through electronic means"*. It integrates science and technological capability across Cyber, EW, SIGINT, and communications to cover continuum of the cyberspace and EM environment. The division applies its capability to support situational awareness of the Cyber and EM environment through reliable and resilient cyber and EW systems including trustworthy ICT, survivable communications networks and systems integration.[23]

26. The CEWD has published the Strategic Plan 2016-2021; it says:[24]

> *Cyberspace is continuing to grow in complexity and dynamism. This is being driven by an increasing demand for mobility, explosion in the number and diversity of networked devices, ubiquitous encryption, escalation of data volumes, and widespread use of software defined systems. These technology trends collectively present significant research challenges to maintain and extend Sigint and Cyber capabilities for access, analysis, exploitation, and defence. Communication networks and wireless capabilities in Cyber are central to this problem space.*

The document also lists *"wireless network characterisation and vulnerability research"* as a priority area of investment under the Cyber Sensing and Shaping chapter.[25]

27. **Others**. Asian countries other than Israel have not achieved the technological threshold in this field to merit a mention. However, not much information is available on Israel cyber & EW doctrine/strategy/road maps, despite the fact that they are the world leaders in some cutting edge technology in this domain, especially the EW. In Jun 2015 Israel announced that it will raise a unified cyber command,[26] but later, in May 2017 it shelved the plans,[27] for reasons not yet known. Even the IDF (Israel Defence Force) Strategy-2015 document[28] mentions electronic warfare in the passing,[29] and includes just about 10 lines towards developing cyber warfare capabilities,[30] which is surprising, to say the least.

EXPLOITING/DEFENDING THE EMS

Exploiting the EMS for Cyber Warfare

28. Mobility demands wireless connectivity, and that is where the technology is moving, whether in civil or in military networks/applications/devices; exploitation of EMS for cyber war is facilitated by such environment. The primary aim of such an exploitation is to infiltrate a computer system/network and inject it with malware to carry out CNE and/or CNA; it could also aim to capture raw RF signal and analyse it offline to extract information, or to re-feed a doctored RF signal back into the system for deception etc. A new expertise is now emerging in this domain- a methodology to force the system (after being injected with a malware)) to transmit data to external devices using covert channels such as ultrasound waves, fan speed, heat signature, LED blinking etc. While some (like the DRFM or hacking into a protected Wi-Fi connection) are fairly mature technologies, others like data exfiltration through covert channels are still at experimental stage and are yet to be commercialised.

(a) Data Spying/Leakage Through Wireless Connections. Probably the most common method of spying on data is getting access through the traditional wireless connections like the WiMAX, wireless IP radios, Wi-Fi, Bluetooth, air interface of the cellular connection (cell phone to the tower), etc. Since all such protocols are well defined and the information is available in public domain, it is simpler to design hacks for them, although encrypted channels certainly pose a

larger challenge. Eg Wireless Aerial Surveillance Platform, or WASP, a US Army spy drone measuring over 6-feet in length and wingspan, has been modified to make it more useful for hacking by equipping it with the tools to crack Wi-Fi network passwords using Back Track Linux (equipped with a full suite of digital forensics and penetration testing tools). WASP can also act as a GSM network antenna enabling it to eavesdrop on calls/text messages made over that network by any phone deciding to connect through it.[31]

(b) Air Injected Malware. There is also the possibility of injecting a malware over the wireless channel (at least the open channels if not encrypted ones). An anti-drone rifle was unveiled during a military exercise by Iran's army in Dec 2016. It is described as "a drone jammer, a portable electronic device used for deflecting the hostile flying objects." The drone jammer can lock onto an enemy drone, and then "disrupt its operation or even hack the aircraft and force it to land safely." On the other hand, the Army Cyber Institute at West Point, USA, has built an antenna-and-computer rifle that can feed information into an open channel of an unlocked drone. This allows the cyber rifle to send an override code to the drone, causing it to crash.[32] Such cyber rifles were also allegedly used by Russia against Ukrainian and Syrian drone attacks.[33] Basic malware injection through a wireless radio link

(c) DRFM. DRFM is an electronic method for digitally capturing and retransmitting RF signal. DRFMs are typically used in radar jamming, although applications in cellular communications are also becoming common. A DRFM system is designed to digitize an incoming RF input signal at a frequency and bandwidth necessary to adequately represent the signal, then reconstruct that RF signal when required. The most significant aspect of DRFM is that as a digital "duplicate" of the received signal, it is coherent with the source of the received signal, and there is no signal degradation. DRFMs present a significant obstacle for radar sensors. A DRFM may modify the signal prior to retransmitting which can alter the signature of the false target, adjusting its apparent radar cross section, range, velocity, and angle. The DRFM digitizes the received signal and stores a coherent copy in digital memory; when needed, the signal is replicated and retransmitted. Being a coherent representation of the original signal, the transmitting radar will not be able to distinguish it from

other legitimate signals it receives and processes as targets. Slight variations in frequency can be made to create Doppler (velocity) errors in the victim receiver as well. Current commercial off-the-shelf (COTS) DRFM systems are capable of receiving analog signals, converting the analog signal to a digital signal, processing and manipulating the digitized signal, and converting the modified signal back to an analog signal for transmission in less than 39 nanoseconds.[34] DRFM systems have the ability to manipulate captured signals at the bit level once the signal has been converted from analog to digital. This ability to manipulate individual bits inside of a signal is a potent capability that wasn't feasible a decade ago. A DRFM system is used to conduct a so-called man-in-the-middle attack (MITM) against a targeted RF receiver. In an MITM attack, an attacker has the ability to alter traffic in a communications channel by injecting themselves into the communications channel between the transmitter and intended receiver. Since the bits can be manipulated, the target receiver can be fooled either through preamble/synchronisation bit manipulation (that will cause loss of synchronisation) or by manipulating the traffic bits (which will cause receiver to get a garbled/doctored message).[35] The US Army and Navy are already using DRFM systems (from M/s Mercury Systems, USA) to bolster their intelligent jamming and deception capabilities.[36,37] DRFM-based systems can also be used to capture the electromagnetic signatures of enemy aircraft, ships, and other units; these electromagnetic signatures can provide intelligence about the capabilities of enemy aircrafts, ships and types of electronic systems in operation. The technology is catching fast, and the global market valued at USD 614 Million in 2016, is projected to reach USD 1,222 Million by 2022.[38] The famous Senior Suter technology developed by the Big Safari unit of the US Air Force is said to be the basis of today's DRFM systems. As the US magazine Air Force Technology puts it:[39]

> *Suter beams electronic pulses into the radar antennas that effectively corrupt, if not hijack, the processing systems that present the enemy operators with their physical picture of the battlefield. Unlike classic jamming or EMP attacks, these data streams do not flood enemy electronics with excess 'noise' or power, but instead insert customised signals, including specialised algorithms and malware, into the vulnerable processing nodes. Continuing*

the viral analogy, network invaders can then extend their 'e-tack' from network to network until they reach the target's communications loop. Whether the network is wireless or wired doesn't matter thereafter.

(d) Data Leakage Through Unintended EM Radiations. The history of data leakage through unintended EM Radiations (EMR), and the protection against it, goes back to the TEMPEST (acronym for *Telecommunications Electronics Material Protected from Emanating Spurious Transmissions or Transient Electromagnetic Pulse Emanation STandard*) project of the National Security Agency (NSA) of USA.[40] It has been proved that unintended EMR from digital devices such as those from the computer/TV screen, data cables, electric cables, keystrokes, etc can be monitored and the content can be reconstructed.[41] TEMPEST monitoring equipment include various kinds of sensitive receivers, which can monitor a wide range of frequencies, and a combination of hardware and software that is capable of processing the received signals into the original data. The data that is picked up is often corrupted by things such as external EMR interference, signal weakness over distances and partial transmission. Advanced algorithms can help provide a more complete picture of the original data. Such an approach typically works across few 100 meters of distance between the target machine and the receiver.

(e) Data Exfiltration Through the Air Gap. Organisations like military, intelligence agencies, critical infrastructure operators, corporates, banks, etc store and process sensitive information within their computer networks. Naturally, such networks are the preferred targets of (military or business) adversaries due to the valuable information they hold. Regardless of the level of protection, a persistent attacker will eventually find a way to breach a computer network connected to the Internet. Consequently, if a network stores sensitive or classified information, an 'air-gap' approach is often used to prevent such a breach, like the one being followed by the Indian Army also. While the cyber security people world over are fixated with preventing ingress into their systems, a cyber researcher, MordechaiGuri, at the Ben Gurion University in Israel, is giving sleepless nights to them by devising ways to exfiltrate computer data to another nearby device via the noise its internal fan generates, by changing air temperatures in patterns that the receiving computer can detect with thermal

sensors, or even by blinking out a stream of information from a computer hard drive LED to the camera on a quadcopter drone hovering outside a nearby window.[42] The team has even shown that they can pull data off a computer protected by not only an air gap, but also a Faraday cage designed to block all radio signals. However, the assumption here that Guri makes is that the computer is already infected with the customised malware, through a USB drive etc, which is probably not preposterous, going by the history of how the highly targeted malware like the NSA's Stuxnet and Flame penetrated air-gapped Iranian computers a decade ago, and how Russia's "agent.btz" malware infected classified Pentagon networks around the same time. There could also be a deliberate supply chain infection to insert the malware. The team has also revealed a magnetic field based approach where the processor operations are coordinated (by a malware) to produce electric currents of certain frequencies, using which their malware can generate a pattern of magnetic forces powerful enough to carry a small stream of information to nearby devices, like a smartphone (loaded with a customised application called ODINI, developed by the same team); the data rates demonstrated are up to 40 bits per second, which is good enough to steal a password or an encryption key over few minutes. Guri's team has also developed a malware that turns a computer's video card into an FM transmitter to capture keystrokes. These malwares go by interesting names such as the US Bee, Disk Filtration, Bit Whisper, Air Hopper, Fansmitter, etc.[43] Researchers at the Fraunhofer FKIE (Fraunhofer Institute for Communication, Information Processing and Ergonomics) Germany, have develop a malware prototype which is able to communicate using inaudible audio signals- allowing it to exchange data even between infected machines lacking a network connection.[44] Based on technology originally designed for underwater communications, the use of ultrasonic frequencies allows the penetration of "air gaps" sealing computers from the outside world. The malware uses built-in microphones and standard speakers to transmit small amounts of data from distances of nearly 20m at up to 20 bits per second- a distance it can enlarge by creating an "acoustic mesh network" out of infected devices repeating the audio signals.

(f) High Energy Electro Magnetic Pulse (EMP). An EMP, also sometimes called a transient electromagnetic disturbance, is a short burst

of electromagnetic energy. Such a pulse's origination may be a natural occurrence or man-made and can occur as a radiated, electric, or magnetic field or a conducted electric current, depending on the source. EMP interference is generally disruptive or damaging to electronic equipment, and at higher energy levels a powerful EMP event can damage even physical objects such as buildings and vehicles. Although it cannot be classified as a true cyber war action, but the final impact is that a computer is rendered non effective by burning the electronics inside- and hence EMP is included in this paper. Weapons have been developed to deliver the damaging effects of high-energy EMP; amid all the recent fears about North Korea building an electromagnetic-pulse weapon that could disrupt America's electronic backbone, another potential threat has been ignored: Russia's new Alabuga EMP weapons program[45]; Russian media describes a program that appears to be aimed at developing tactical EMP weapons that would affect a small area. Such weapons could be used to create a devastating effect on the enemy. Eg an EMP bomb exploded over a city could neutralise the power grid and create chaos, or it could "burn out' all electronic devices including mobile phones, traffic light systems, etc.

Battle Field Scenarios for Exploitation the EMS

29. As already discussed, the battle field networks are transiting to complete IP networks (backbone voice/data/video networks, CNR etc), with a large component of wireless connectivity. Apropos, there is ample opportunity available in the battle field for exploitation of EMS to conduct cyber warfare. Some of these scenarios are given below.

(a) Use of an airborne weapons system to deliver malicious code into cyberspace via a wireless radio connection.

(b) Intercepting and recording computer data from a Wi-Fi connection, and post offline analysis, use the same to infer enemy information.

(c) Entering an SDR network using spoofed IP, and meddle with control signals to disrupt the CNR, or to display false GPS reading, or even send misleading messages to enemy soldiers.

(d) Feeding doctored signals to radar antenna (using DRFM techniques) to present false screen displays and avoid detection of own aircrafts/drones.

(e) Establishing a fake BTS tower to force enemy cellular phones to log on, and thereafter passively monitor the voice conversations, read SMS, emails and all data that the user is transmitting through his phone.

(f) Bringing down a drone (electronically) through use of anti-drone rifle.

(g) Jamming the radio channels of a computer network, either in the backbone (WiMAX, IP radio etc), or in the last mile access (Wi-Fi, Bluetooth, Zigbeeetc). This would render the computers unable to communicate with each other, and thereby collapsing the network.

(h) A very simple way to enter into enemy mobile network is to have a SIM card of enemy network. A number of enemy BTS are located close to the border areas, where one can log into the target network. Thereafter, messages, mails as deemed suitable may be sent to designated target phones, or as a broadcast, as part of a larger deception plan.

30. Other techniques like the TEMPEST, or the ones developed by Israeli scientist Guri are applicable across very short ranges (at least as of now), and are thus more suited to scenarios like clandestine operations, spying on embassies, etc.

Defending the EMS

31. From the foregoing discussion it is amply clear that with the traditional boundaries between telecom and IT blurring, there is enough opportunity to exploit the EMS for conduct of cyber warfare. More so in the tactical battle field because unlike strategic networks which are mostly terrestrial, the military networks (due to reasons of quick deployment/wrap-up and mobility) are mostly dependent on wireless connectivity.While we endeavour to mature technologies and innovations to exploit the EMS to our advantage, we must not forget that

the same is true of our adversaries also. It is therefore no less important to employ measures to defend the EMS against this exploitation.

32. While traditional EP measures are well known like minimum transmission, secure transmission, low power, directional antenna, frequency hopping signals, etc, there is a need to employ new technologies to guard the spectrum against possible exploitation for cyber warfare. To be able to conduct effective cyber warfare (CNE or CNA) it is necessary that the attacker reaches bit level information contained in the RF signal so that he can manipulate the same or injecteda malware. Apropos, (in addition to making the access to EM signal itself difficult), it should be our endeavour to make it more and more difficult for the attacker get down to the baseband level bit stream. Some suggestions to minimise exploitation of EMS for cyber warfare are discussed below.

(a) Minimise Transmitted Power. This is a very basic precaution in any wireless transmission. Depending on the communication range required, and the environment conditions, the RF transmitted power should be kept at bare minimum. Nowadays, almost all wireless transmitters come equipped with the Adaptive Power Control feature and the same should be enabled.

(b) Directional Antenna. It is always preferred to use a directional antenna over an Omni-directional antenna, unless necessitated by the operational requirements (like a tactical CNR).This will ensure that the RF spillage over enemy territory is minimal, and at the same time transmitted power is also optimised.

Minimise Transmission Time. Radio operators should be trained to transmit for the minimum time required and avoid over usage.

(c) Spread Spectrum Techniques. Direct Sequence Spread Spectrum (DSSS) and frequency hopping (FH) techniques can spread the signal over a wide frequency range, and even spread it below the RF noise floor (by using DSSS). Such techniques which are fairly mature today can minimise the detection of RF signal itself.

(d) Application Layer Encryption. When we operate in the IP domain, one of the simpler technique is to use application layer encryption; eg the type of encryption used by WhatsApp etc. The bigger the encryption key, the longer it will take to break it.

(e) IP layer Encryption. In addition to above,IP layer encryption (IPSEC) should be enabled in all IP devices/networks. This will add one more layer of difficulty.

(f) Encryption at Physical Layer. Finally the traditional secrecy/ encryption device kicks in which will encrypt the signal just before it is transmitted.For highly secret messages one could also include manual encryption methods like the OTP (One Time Pad).

(g) Proprietary Handshake. Proprietary handshake mechanisms will prevent MITM type of attack, and prevent an imposter to masquerade as a genuine user of the network.

(h) Bit Interleaving Techniques. Interleaving techniques are very commonly used in digital microwave transmissions. Since these mechanisms are vendor proprietary implementations, and combinations are almost infinite, it is very difficult to de-interleave a bit sequence through brute force methods.

(i) Steganography. Sensitive messages could be hidden inside an image, a technique known as Steganography. Only the authorised recipient would be able to decode and extract the text message from the image.

(j) Shielding. Shielding of devices from EMR is achieved by a number of methods. The most sophisticated devices use advanced micro-components that have been designed from scratch to minimize TEMPEST emanations. Generally, shielding involves encompassing the device in a Faraday cage that does not permit stray emanations, along with special modifications to the power source. This usually involves a heavy metal case around an object. TEMPEST shielding also involves

such issues as the design of a room and placement of equipment within it, to ensure that no information can escape.

CONCLUSION

33. As is evident from the foregoing discussion,technology enables exploitation of EMS for cyber warfare. The fact that military networks in the tactical battle field are primarily wireless, makes the scenario more grim. It's only a matter of time before technologies like the ones developed by Guri and his team become mature and are commercially availableoff the shelf. With even newer concepts like the IoT becoming a reality,it's a matter of not more than next 5-10 years that the same proliferates in military networks also.The threat is real, it's here to stay; we might as well learn to live with it, and while developing offensive capability do not overlook the fact that we are equally vulnerable, and need to protect the EMS through technology and innovative thinking.

References

1 Mann Col Edward, USAF, 1994,*Desert Storm: The First Information War?* , Aerospace Power Journal - Winter 1994 (http://www.iwar.org.uk/iwar/resources/airchronicles/man1.htm) Accessed 24 Aug 2018

2 Fulghum David A. and Wall Robert, 2007,*Israel Shows Electronic Prowess: Attack On Syria Shows Israel Is Master Of The High-Tech Battle,* Aviation Week & Space Technology Nov 26, 2007 (http://aviationweek.com/awin/israel-shows-electronic-prowess) Accessed 25 Aug 2018

3 Katz Yaakov, 2010, *And They Struck Them With Blindness: A Rare Glimpse Into Israel's State-Of-The-Art Electronic Warfare Capabilities,* (http://www.jpost.com/Magazine/Features/And-they-struck-them-with-blindness) Accessed 25 Aug 2018

4 http://gentleseas.blogspot.com/2007/10/suter-jamming-our-good-guys.html, Accessed 26 Aug 2018

5 Details of DRFM are discussed later in this paper

6 https://www.airforce-technology.com/features/feature1669/, Accessed 26 Aug 2018

7 Available at https://info.publicintelligence.net/USArmy-CyberContest-2.pdf, Accessed 22 Aug 2018

8 Available at http://mattcegelske.com/wp-content/uploads/2013/03/Information_Dominance _Roadmap_March_2013.pdf, Accessed 22 Aug 2018

9 http://idstch.com/home5/international-defence-security-and-technology/cyber/integrated-cyber-electronic-warfare-signals-intelligence-and-communications-operations-for-future-battlefield/, Accessed 25 Aug 2018

10 Ibid

11 https://www.army.mil/article/171596/army_announces_arcyber_as_an_ascc, Accessed 25 Aug 2018

12 Available at https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN3089_FM%203-12%20FINAL%20WEB%201.pdf, Accessed 22 Aug 2018

13 Cole Harold T, Cdr, US Navy, 2014, *Warfare In The Electromagnetic Spectrum And Cyberspace: United States Air Force Cyber/Electromagnetic Warfare Command Construct* (http://www.au.af.mil/au/awc/awcgate /cst/bh_2014_cole.pdf) Accessed 25 Aug 2018

14 SharmaDeepak, 2010, *Integrated Network Electronic Warfare: China's New Concept of Information Warfare*, Journal of Defence Studies: Vol 4. No 2. April 2010, published by Institute for Defence Studies and Analyses, New Delhi (https://idsa.in/jds/4_2_2010_ChinasNewConceptofInformationWarfare_dsharma) Accessed 22 Aug 2018

15 Sharma Deepak, 2011, *China's Cyber Warfare Capability and India's Concerns,* Institute for Defence Studies and Analyses, New Delhi (https://idsa.in/system/files/jds_5_2_dsharma.pdf) Accessed 22 Aug 2018

16 Costello John, 2016, *The Strategic Support Force: China's Information Warfare Service,* China Brief, Volume: 16 Issue: 3, Jamestown Foundation (https://jamestown.org/program/the-strategic-support-force-chinas-information-warfare-service/) Accessed 22 Aug 2018

17 https://thediplomat.com/2017/04/pla-strategic-support-force-the-information-umbrella-for-chinas-military/, Accessed 25 Aug 2018

18 https://www.rand.org/pubs/research_reports/RR2058.html, Accessed 25 Aug 2018

19 Costello John, 2015, *Chinese Views on the Information "Center of Gravity": Space, Cyber and Electronic Warfare*, China Brief, Volume: 15 Issue: 8, Jamestown Foundation (https://jamestown.org/program/chinese-views-on-the-information-center-of-gravity-space-cyber-and-electronic-warfare/) Accessed 22 Aug 2018

20 GilesKeir, *The Next Phase Of Russian Information Warfare,* NATO Strategic Communications Centre of Excellence: p 13 (https://www.stratcomcoe.org/

next-phase-russian-information-warfare-keir-giles) Accessed 21 Aug 2018

21 Freedberg Sydney, 2015, *Army Fights Culture Gap Between Cyber & Ops:Dolphin Speak,* Breaking Defense, 10 November 2015,(http://breakingdefense.com/2015/ 11/army-fights-culture-gap-between-cyber-ops-dolphin-speak/) Accessed 20 Aug 2018

22 Independent, 22 Feb 2017(http://www.independent.co.uk/news/world/europe/russia-military-information-warfare-hacking-allegations-a7594456.html) Accessed 20 Aug 2018

23 https://www.dst.defence.gov.au/research-division/cyber-and-electronic-warfare-division, Accessed 25 Aug 2018

24 Australian Government, Department of Defence CEWD Strategic Plan 2016-2021: p 21 (https://www.dst.defence.gov.au/sites/default/files/divisions/documents/CEWD_Strategic_Plan_2016-2021.pdf) Accessed 23 Aug 2018

25 Ibid: p 22

26 The Times of Israel, 16 Jun 2015 (https://www.timesofisrael.com/army-to-establish-unified-cyber-corps/) Accessed 27 Aug 2018

27 The Times of Israel, 14 May 2017 (https://www.timesofisrael.com/army-beefs-up-cyber-defense-unit-as-it-gives-up-idea-of-unified-cyber-command/) Accessed 27 Aug 2018

28 English translation available at https://www.belfercenter.org/sites/default/files/files/publication/IDF%20doctrine%20translation%20-%20web%20final2.pdf, Accessed 27 Aug 2018

29 Ibid: p 9

30 Ibid: p 44

31 https://climateviewer.com/2014/01/18/nsa-tempest-attack-can-remotely-view-computer-cellphone-screen-using-radio-waves/, Accessed 25 Aug 2018

32 https://www.popsci.com/iran-anti-drone-rifle, Accessed 05 Jul 2018

33 https://www.militaryaerospace.com/articles/print/volume-27/issue-8/special-report/today-s-battle-for-the-electromagnetic-spectrum.html, Accessed 26 Aug 2018

34 http://magazine.milcyber.org/stories/physicallayerjammingthreats, Accessed 22 Aug 2018

35 Ibid

36 Keller John, 18 Jun 2014, *Navy And Air Force Choose DRFM Jammers From Mercury Systems To Help Spoof Enemy Radar* (https://www.militaryaerospace.com/articles/2014/06/mercury-drfm-jammer.html) Accessed 23 Aug 2018

37 Keller John, 29 Jun 2018, *Mercury Wins Nearly $29 Million In DRFM-Based Electronic Warfare (EW) Work Within One Week's Time* (https://www.militaryaerospace.com/articles /2018/06/electronic-warfare-ew-drfm-radar-spoofing.html) Accessed 23 Aug 2018

38 https://www.marketsandmarkets.com/PressReleases/drfm.asp, Accessed 23 Aug 2018

39 https://www.airforce-technology.com/features/feature1669/, Accessed 26 Aug 2018

40 https://www.sans.org/reading-room/whitepapers/privacy/introduction-tempest-981, Accessed 24 Aug 2018

41 https://climateviewer.com/2014/01/18/nsa-tempest-attack-can-remotely-view-computer-cellphone-screen-using-radio-waves/, Accessed 25 Aug 2018

42 GreenbergAndy, 02 Jul 2018,*Mind The Gap: This Researcher Steals Data With Noise, Light, And Magnets*

(https://www.wired.com/story/air-gap-researcher-mordechai-guri/) Accessed 23 Aug 2018

43 Kumar Mohit, 2017, *Hacker Can Steal Data from Air-Gapped Computers Using IR CCTV Cameras*(https://thehackernews.com/2017/09/airgap-network-malware-hacking.html) Accessed 21 Aug 2018

44 Snyder Bob, 2013, The Ultrasonic Based Malware (http://www.it-sp.eu/index.php?option=com_ content&view=article&id=1778:the-ultrasonic-based-malware-&catid=38:security&Itemid=74) Accessed 22 Aug 2018

45 http://nationalinterest.org/blog/the-buzz/forget-north-korea-russia-now-building-emp-weapons-23760, Accessed 25 Aug 2018