CENTRE FOR JOINT WARFARE STUDIES

Aligned with the Future ★ Victory through Joint Knowledge ★

SYNODOS PAPER | VOL - XII NO-19 / SEP 2018

CYBERTRONIC WARFARE- BEWARE THE MONK !

Lt Gen Rajesh Pant, PVSM, AVSM,VSM (Retd), PhD is an internationally renowned Techno-Scholar-Warrior and Mentor.

The officer served the Indian Army Signals for more than four decades. In his last assignment he was the head of the Indian Army's Cyber Security training establishment at Mhow. He has undergone EW training in Hungary and has also participated in many military operations, including in Sri Lanka and Kargil

As a scholar, the officer is a triple post graduate, with MTech from IIT Kharagpur on Satellite Communications & Remote Sensing, MPhil from Chennai University on National Security and Master of Management Studies from Osmania University. In June 2014, the officer also obtained his PhD in the important field of Information Security.

The more technology we add to ensure Cyber Security, the lower the fruit hangs for cyber criminals

ABSTRACT

*An extrapolation of modernisation trends in the defence forces clearly indicates a shift towards greater digitisation, drones and unmanned systems, battlefield management systems, precision munition guided by indigenous navigation systems, Geographical Information Systems, militarisation of space, use of Artificial Intelligence, Deep Learning, Data Analytics, cyber warfare capabilities and soldier-as-a-system as some of the technologies that would transform the future battlefield. However, all these aspects are heavily dependent on electronic components, software applications, digital storage and networked communications. This has created a deadly new threat termed as **Cybertonic Warfare**, which is a convergence of the existing domains of Cyber and Electronic Warfare. This new combat threat can be referred to as the MONK or the Mother-Of all- Non-Kinetics.*

The author is the global founder and propagator of this modern threat and in this paper he will outline the various components and vectors of Cybertronic Warfare

Introduction

Towards the end of the last century, Dr Martin Libicki of the National Defence University in Washington USA, had written a seminal paper titled 'What is Information Warfare?'. In this article, seven different forms of Information Warfare (IW) had been enumerated which also included Cyber Warfare. However the concept of Cyber Warfare at that point of time was a futuristic form of warfare involving robots and virtual reality such as in the realm of science fiction and all that was not covered by the other six forms of Information Warfare (in which there was some clarity). Over a period of years and with the advent of computer networks as also the proliferation of the internet, Cyber Warfare (CW) as known and understood today involves the deliberate insertion of a malware so as to result into soft or hard attacks on a target through interconnected computer or smartphone networks.

Non kinetic warfare implies the degradation or destruction of enemy's combat potential through non-physical means (as against bullets and bombs). The other form of non-kinetic warfare prevalent today is termed as Electronic Warfare (EW), which involves passive and active measures conducted in the Electro-Magnetic (EM) spectrum. The definition and interpretation of this type of warfare has by and large remained consistent since the past five decades. However, a deadly variant of Electro Magnetic Spectrum Operations in the form of Directed Energy Weapons (DEW) has now been added into this warfare which has the potential to be a game changer in the conduct of military operations in the modern digital battlefield. The end result of EW also conforms to either gaining actionable intelligence or ensuring soft or hard destruction of the end user equipment through either Jamming or the use of DEW respectively.

In the modern era of convergence of services into a common platform, and considering that the desired end result of both CW and EW is similar, the author is propagating a new domain of warfare titled ***Cybertronic Warfare.*** This is the converged domain of CW and EW, and as we shall examine in due course, it has the potential to create the battle winning factor in a conflict situation and thus earn the title of MONK or Mother-Of-all-Non-Kinetics.

What is Cybertronic Warfare?

Unlike an android game app with a similar name, this real world domain of warfare termed as Cybertronic 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** and can be defined **as all military 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.**

Key features of CeW as emerging from the above definition are as under :-

(a) It is a military action, which can be conducted at strategic, operational or tactical levels, in coordination with the operational plans.

(b) 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.

(c) In it's passive avatar, CeW provides a source of intelligence.

(d) 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 through DEW.

(e) It includes the preventive measures against CeW conducted by the adversary on own systems.

The Cybertronic Process

Having understood the basics of CeW, we will now examine the various vectors which will be employed for the conduct of such an operation. These attack vectors will by and large follow the following sequence of events:-

(a) Analysis of known information of hostile network, battlefield management systems and frequency bands of operation of wireless links in the geographical area of interest.

(b) Scanning of the EM spectrum in the band of interest.

(c) Analysis of signals, including their demodulation and demultiplexing.

(d) Synchronsiation, deinterleaving, decryption and extraction of data or IP traffic depending on type of transmission.

(e) Deciding on whether to either obtain intelligence through passive means, including Direction Finding, or employment of attack vector.

(f) Deciding attack vector of either malware insertion or Jamming or use of Directed Energy Weapon as per operational plans.

(g) For malware insertion, carry out the cyber warfare stages of scan, insert, lateral spread, execute and extricate.

(h) For perception management, insert the approved theme into the target cyber domain.

(j) For Jamming, use of EW jammer against target radar/receiver

(k) For Directed Energy weapon, employment of High Power Microwave Pulse from suitable platform.

(l) Damage assessment.

(m) Preventive measures against CeW by the adversary.

CeW Case Studies

Operation Orchard was an Israeli airstrike on a suspected nuclear reactor in the Deir ez-Zor region of Syria, which occurred just after midnight on September 6, 2007. The Israeli and US 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:-

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

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

(c) 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.

(d) 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.

(e) **Perception management** was conducted to mislead the Syrian commanders.

Operations On UAVs: Iran 2011, South Korea 2012, Russia 2014. India 2017. On 4 December 2011, an American Lockheed Martin RQ-170 Sentinel unmanned aerial vehicle (UAV) was captured by Iranian forces near the city of Kashmar 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, after initial reports from Western news sources disputedly claimed that it had been “shot down”. The United States 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. And recently in 2017, an Indian UAV was suspiciously brought down near the border with China.

In all these cases CeW was reportedly conducted as under :-

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

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

(c) Jamming was conducted on the original GPS frequency.

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

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. Russian Special Forces managed to derail all important communications systems through direct physical impact on them by combined field and high-tech operation. One of the techniques used by the Russians for cyber espionage was the "Snake", also known as Uroburos. The use of Uroburos, along with the physical attacks against networks therefore combined both "old school" operations with modern cyber warfare techniques to gain the desired impact. In this case an element of the classic Anti-neck **Command and Control Warfare** was also employed along with **EW and CW to create the 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 built on digital technologies by Russia, is designed to defend against the attack on command posts, force groupings, industrial and administrative facilities. The system suppresses the functioning of electronics-powered stationary and mobile objects with the help of interference effects in what is described as "smart" 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. This is another example of a **converged CeW weapon system.**

Cybertronic Technologies

To effectively implement EW, the operator needs to understand both the latest communication and radar technologies (which are his target), as also have a clear knowledge of EW equipment and techniques for undertaking EW operations. In addition he should also know the counter measures against hostile EW actions. Similarly in CW, there is a need to understand the intricacies of computer programming and networks (which are the target), as also the intrusion detection and prevention systems for own systems. As evident, the spectrum of technologies in CeW is vast and due to constraints of space, only a few key technologies will be discussed herein.

MANET. In the Tactical Battle Area, state-of-the-art communications are based on networks which emanate from the soldier and include the sub units, units, the formation headquarters of brigade and division upto the corps headquarters. Such networks are based on MANET or Mobile Adhoc Networks provided through a Software Defined Radio(SDR). These radios can either be used in the walkie-talkie mode or in the MANET mode. Since these radios are utilising the Internet Protocol (IP), they can be configured to act as routers whereby their ranges can be increased through a number of hops. However, they suffer from a restriction of latency, which is the time lag between the stimulus and the response. This is a critical factor in the tactical scenario in situations such as fire support and thus the number of hops is restricted.

Mobile Cellular Tactical Communication Networks. This is basically divided into the Radio Access Network (RAN) and the Evolved Packet Core (EPC). In the RAN, the User Equipment (UE), be it the radio or a hand held terminal or a sensor or any such device, is connected to the base station which in the latest 4G technologies of Long Term Evolution (LTE) is called the Evolved Node Broadband or eNodeB. This communication media is based on wireless technology and may also include the usage of Multi Input Multi Output or MIMO antennas for improved performance. This eNodeB is further connected to the EPC which comprises of Mobility Management Entity (MME), Serving Gateway and the Core Network via the IP network which is based on broadband media of either Optical Fibre Cable (OFC) or Microwave (terrestrial or satellite based) communications.

5G. Future cellular networks with atleast 100 times better parameters than 4G are to be based on Software Defined Networks and Network Function Virtualisation. The brain of this fifth generation wireless communication system is based on Big Data Engines and drivers which includes Artificial Intelligence (AI). The reader may well be aware of the IEEE standards in this field. IEEE 802.11 pertains to the Wireless LAN and is controlled by the WiFi Forum. IEEE 802.16 pertains to Wireless MAN and is controlled by the WiMAX Forum. Similarly IEEE 802.15 pertains to 5G standards which is presently being coordinated by an industry alliance.

Signal Analysis, Modulation and Multiplexing. In the EW phase of the Cybertronic process, the operator must be aware of the various technologies used for multiplexing of a number of input digital signals into a bit stream or IP packets and how these are modulated with a carrier wave to facilitate the Radio Frequency (RF) transmission. As a thumb rule, the 3dB RF bandwidth of a signal is approximately twice the bit rate of the signal and can provide a crude initial estimate in the interception process. While 16/64 QAM type of modulations are in vogue, the aspects of Phase Shift Keying (PSK) and Frequency Shift keying (FSK) are also important in digital modulations. Similarly the Time Division or Frequency Division Multiplexing concepts and the IP packetisation formats are very important for obtaining the subsequent intelligence. Radar signals are based on the reflection obtained from a pulsed digital transmitted wave and it is mandatory to know the aspects of Pulse Repetition Frequency, Image Processing etc as also the transmission technologies of radar so as to be able to analyse the Radar signals.

Deep Packet Inspection (DPI). Shallow packet inspection **(SPI)** examines the headers of the packets (which is the information placed at the beginning of a block of data, such as the sender and recipient's IP addresses), as opposed to the body or "payload" of the packet. This kind of packet inspection allows the communications to remain 'virtually anonymous' since the content of the packets is not observed, and the information in the header is used only to route the packet. Medium Packet Inspection **(MPI)** is typically used to refer to 'application proxies', or devices that stand between end-users' computers and ISP/Internet gateways. These proxies can examine packet header information against their loaded parse-list. When a packet enters the proxy, it is analyzed against a parse-list that system administrators can easily update. A parse-list allows specific packet-types to be allowed or disallowed based on their data format types and associated location on the Internet, rather than on their IP address alone. Deep Packet Inspection **(DPI)** is a technology that enables to analyse internet traffic, through the network, in real-time and to differentiate them according to their payload. DPI now allows the EW interceptor to scan the payload of IP packets as well as the header and thus precisely identify the origin and content of each packet of data that passes through the networking hubs.

Direction Finding(DF). The basic concept of DF is to obtain the azimuth of the target from various different locations and then create a Circular Error of Probability (CEP) to fix the target location. In case of radars, the intersection of the azimuth and the elevation is utilised to fix the target location using narrow beam antennas. Common DF techniques include the Watson-Watt, Doppler DF, Time Difference of Arrival and Interferometry. An elaborate procedure for calibration is required for the DF equipment prior to use and in order to obtain accuracies of about one degree RMS it is important to ensure the proper siting of DF equipment.

Jamming. In both communication and radar jamming, the basic concept is that the Jammer to Signal (J/S) ratio at the target receiver should be greater than the required Signal to Noise Ratio. Typically a white or pink noise signal is used for jamming. Another jamming technique is termed as Imitative (for communication) or Deceptive (for radar) jamming where in the latter case it deliberately causes errors in the range or angle tracking. The J/S reduces as the range reduces and the Burn through range is that at which the J/S is no longer adequate.

Electronic Protection in Modern Radars is achieved through the use of ultra-low side lobes, side lobe canceller, side lobe blanker, anti -cross polariser, monopulse, compression, anti–doppler pulloff, frequency range-gate correlation, anti-chaff, leading edge tracking, anti-AGC jamming, frequency agility, PRF jitter and Home-on jam modes.

Directed Energy Weapons (DEW). The use of a non-nuclear high powered microwave source to generate an **Electro-Magnetic Pulse (EMP)** lies in the category of DEW. These are the ultimate non-kinetic weapons of the future as it can be employed to literally fry out the electronic components from a distance. Underground Command and Control Systems can also be destroyed using either front door or back door coupling (through generators or power cabling). All CMOS components, computers, Local Area Networks, Power Supplies etc are targeted by this pulse. Permanent damage occurs if the RF pulse is at a field strength of 2 KV/m, even if the equipment is off. The pulses are found to be more effective in the frequency range of 1-3 GHz, and they can be employed either in the ground based Air Defence role or in the offensive role from an aerial platform. To generate an energy of 1 KV/m at one Km, a power of 10 GW is required and that is where the problem was till now. However scientists have now been able to successfully generate this energy using chemical reactions which then convert to electrical energy. Another application of DEW is in the **Laser** band, where the Laser provides a very high accuracy weapon.

Cyber Attacks. While the end result may vary from system crashes to ransomware, the following are the key technologies used in cyber attacks :-

(a) **IP Spoofing**. The intruder sends messages to a host with an IP address (not its own IP address) indicating that the message is coming from a trusted host to gain un-authorized access to the host or other hosts

(b) **Routing Attacks**. An attacker could forge a Routing Information Protocol (RIP) packet, claiming his host “X” has the fastest path out of the network. All packets sent out from that network would then be routed through X, where they could be modified or examined. *Onion Routing* is also a technique of hiding the attackers tracks.

(c) **ICMP Attack**. Internet Control Message Protocol (ICMP) is used by the IP layer to send one-way informational messages to a host. There is no authentication in ICMP, which leads to attacks using ICMP that can result in a denial of service, or allowing the attacker to intercept packets.

(d) **Ping of Death Attack.** An attacker sends an ICMP Echo request packet that is much larger than the maximum IP packet size to victim. The victim cannot reassemble the packets and his OS may be crashed or rebooted as a result.

(e) **Packet Sniffing**. Because most network applications distribute network packets in clear text, a packet sniffer can provide its user with meaningful and often sensitive information, such as user account names and passwords

(f) **MAC Address Spoofing**. These attacks involve the use of a known MAC address of another host to attempt to make the target switch forward frames destined for the remote host to the network attacker.

(g) **ARP Attack**. Address Resolution Protocol attack occurs when someone is trying to change the ARP table of MAC and IP addresses information without authorization.

(h) **DHCP Starvation**. A Dynamic Host Control Protocol (DHCP) starvation attack works by broadcasting DHCP requests with spoofed MAC addresses:-

(i) **TCP "SYN" Attack**. This is also known as SYN Flooding. It takes advantage of a flaw in how most hosts implement the TCP three-way handshake.

(j) Man-**in-the-Middle (MitM) Attacks**. The feasibility of mounting a MitM attack on the Secure Socket Layer (SSL) protocol is used by hackers wherein they can either relay or manipulate the data between two users.

(k) **Port Scan Attack**. A Port Scan is one of the most popular reconnaissance techniques attackers use to discover services they can break into.

(l) **Backdoor Attacks**. Some applications may have well-known backdoors or shortcuts that bypass otherwise secure controls and provide unauthorized access.

(m) **Authentication Attacks**. Applications with weak or no authentication are prime targets for unauthorized use and abuse over the network.

(n) **Phishing Attacks**. DNS names can be spoofed or DNS servers can be compromised.

(o) **Access Attacks**. Applications often grant excessive access to resources, allowing unprivileged users excessive access *Cross-site scripting (xss)* attacks take advantage of such vulnerabilities and create exploits for the same in malware.

(p) **DNS Poisoning**. Also called DNS spoofing, it occurs when an attacker is able to redirect a victim to a different website than the address that he types into his browser.

(q) **Buffer Overflows**. When the presentation from the application exceeds or mismatches the required convention at the application layer, unexpected events can occur.

Preventive Measures. CeW also includes the uninterrupted utilisation of own communication, radar and computer networks. Each of these categories have a number of technologies for such countermeasures. In EW the counter measures are classified as ECCM and include the use of chaff, decoys and encryption etc. For computer networks the present concepts include firewalls, Intrusion Detection and Prevention systems, End-point security techniques and anti-virus software. Latest concept to tackle Advanced Persistent Threats is to employ Behavioural Analysis techniques using sand boxing and thus prevent attacks. The author would like to stress on laying emphasis on all the three aspects of Process, Policy and Technology to achieve Cyber Security. Historically, the human factor needs to be addressed with greater seriousness to prevent data breaches.

Need for Integrated Approach for CeW

With nearly four decades of military experience, the author has observed that in most militaries the EW aspects are handled by either the Signals (in India), the Intelligence (in US), the Radio Electronic Combat (in Russia) and so on. These personnel are highly skilled in warfare in the EM spectrum and the EW technologies as enumerated earlier. However, in order to conduct cyber operations, there are still many organisational grey areas and a hesitancy to let it remain an 'All Arms' field. Decision makers need to realise that this sphere requires experts in the field of software programming and its different avatars. Furthermore, the employment of EMP weapons has still not been tasked to any arm. Add to that the fourth difficult task of decryption which requires a mathematical prowess and we have the requirement of a specialised skill that is today not available as a recognised cohesive vertical in any arm or service. The reader would well understand that militaries are structured to fight with full freedom in their entire domain of warfare. Thus to conduct a successful CeW operation it is imperative that a single agency takes the entire operation to it's logical conclusion, rather than 'hand over' a part operation to another agency midway – a dangerous strategy.

Furthermore, with the advent of Internet of Everything and the growing dependence on wireless media in higher frequency bands for networking, it would not be possible to conduct any cyber operation without the added employment of the EM spectrum and use of decryption techniques. It is thus anticipated that this realisation for the necessity of CeW as a domain will lead to the creation of converged units, organisations, training processes and decision making verticals in militaries of the world.

Conclusion

While Dr Libicki in his seminal paper on Information Warfare attempted to segregate the seven key aspects of IW, over a period of time and changing technologies it is evident that the era of convergence is here to stay. Accordingly war fighting techniques are also converging and in this paper the author has propounded the concept, definition and spectrum of the domain of Cybertronic Warfare. The need for a cohesive strategy to conduct and counter the same is the call of the day. Undoubtedly, in days to come it will be the greatest disruptor in the modern digitised battlefield. Beware the MONK !

Disclaimer : Views expressed are of the author and do not necessarily reflect the views of CENJOWS.

CENTRE FOR JOINT WARFARE STUDIES (CENJOWS)
Kashmir House, Rajaji Marg, New Delhi-110 011
Tele. No. : 011-23792446, 23006535, 23006538/9 | Fax : 011-23792444
Website : https://cenjows.gov.in | **E-mail** : cenjows@yahoo.com