In May 2017 a Sukhoi-30 fighter aircraft of Indian Air Force crashed in a remote area of Arunachal Pradesh. Use of a Cyber Weapon by an adversary is being considered as one of the reasons for this mysterious mishap.

In June 2017, the largest shipping container port in India and a nuclear plant in Russia were crippled by a Ransomware attack.

Introduction

Predicting the future battlefield is both an art and a science. While the art of creativity and envisioning the future lies at the base of any such prognostication, many statistical methods exist for forecasting the battlefield of the future. These include extrapolation based on historical facts, time frequency analysis, auto regression, data mining and curve fitting techniques. Furthermore, technology forecasts are fraught with the risk of the entry of a disruptive technology that proves to be a game changer. This is where the strategic and domain expert enters and moderates the crystal gazing exercise to a more practicable level.

The invisible wars of the future have already commenced around the world. While the Gulf War presented one of the initial pictures of the use of Electronic Warfare (EW) as a part of the Shock-and-Awe tactics, the subsequent proliferation of the Internet and computer based networks created the new domain of Cyber Warfare (CW). This domain was extensively employed in the operations in Georgia, Estonia until it was realised that software could also be used for hard attacks. This is when the Stuxnet virus was injected to disable over a thousand nuclear enrichment rods in Natanz, Iran. There was a swift counter to this through the Shamoon
virus which disabled hundreds of computers of ARAMCO Oil Company in Saudi Arabia. The Cyber Wars had begun, and they have continued since then in a number of variants which extend to negatively impacting both the critical and the non-critical infrastructure of the nation state.

Before the dust had even settled on the cyber attacks, came the next game changer - the High Energy Electromagnetic Pulse. This had the potential of causing a range of results spreading from causing burns on a human being to knocking out all electronic systems of a combat platform from a distance. The battlefield was now getting more invisible, less bloodier but with greater damage. This is our point of take off to the environment that would prevail in the tactical battle area of the future.

Electronic Battlefield Systems of Future

A time series extrapolation of modernisation trends in the defence forces of the sub-continent clearly indicates a shift towards greater digitisation, drones and unmanned systems, battlefield management systems, precision munition guided by indigenous navigation systems, Geographical Information Systems (GIS), militarisation of space, use of Artificial Intelligence (AI), Deep Learning, Data Analytics, cyber warfare capabilities and soldier-as-a-system as some of the technologies that would transform the future battlefield.

While our adversary in the North has already reorganised it's command structures into weapon platform based and region based commands, our Western neighbour has created a Cyber Cadre to handle the threats in that domain. Accordingly the picture of the future battlefield emerges as given hereafter.

24 x7 strategic surveillance is carried out with a mix of assets based on satellites, aircrafts, drones and ground based radars. Tactical level surveillance also employs Battlefield Surveillance radars supplemented by ELINT and SIGINT systems and drone mounted cameras. The sensors mounted on all these assets send their outputs via a secure communication wireless network to a Regional or Formation HQ Surveillance Centre, where the technologies of GIS based Change Detection and Data Analytics are used to keep a constant vigil for threat detection. The regional Surveillance Centres are networked with other surveillance centres to prepare a picture that can facilitate the shared awareness.
The processed inputs from the surveillance centres will either be stored in the tactical cloud for retrieval by a pull-down mode or be sent via secure wireless/tactical OFC networks to the Decision Support Centres (DSC). This consists of various sub-systems comprising Operations, Logistics, Intelligence and Terrain which are linked to a networked environment based on the Internet of Everything (IoE). Based on the inputs provided by the various sub-systems at the DSC, the operational commander is given a composite, layered, GIS based graphical situational picture. The entire centre is built around digital electronics.

Decisions from the DSC at the appropriate level are then conveyed to the selected weapon system for kinetic action on the desired target. These are again conveyed as digital information via communication networks. And finally, the weapon platform itself, be it an aircraft, destroyer ship or artillery gun, comprises of it's own sub-system with software and hardware components.

The Achilles Heel of the future battlefield therefore is the software applications, hardware electronic components and the wireless networks. This is the target of Cyber Electronic Warfare, which is the convergence of Cyber and Electronic Warfare. Let us first see these two forms of warfare separately.

**Cyber Warfare (CW)**

CW includes all offensive and defensive actions taken in the Cyber Domain consisting of networked end point devices. A typical modus operandi of the cyber attack involves the stages of Scanning, Entry, Lateral Spread, Control of Victim Device, Exploitation and Exfiltration. The software code devised for entry through a vulnerability is termed as an 'exploit', and the attack path is termed as 'attack vector'. A Zero Day Attack is one for which the preventive patch has not been implemented.

The intent of CW is to insert a malware into the computer system which when activated can perform a range of mischievous functions as per some examples given below :-

(a) Distributed Denial of Service Attack which would prevent the computer system from performing any action or information exchange. This would imply making the system non-functional, thereby ceasing all decision support activities in a Command Center.
(b) eBomb attack which on activation would prevent a weapon from acquisition of target parameters and seize firing.

(c) Worm attack on the Supervisory Control and Data Acquisition (SCADA) System of a nuclear plant, power and communication grids to cause physical damages and outages.

(d) Ransomware attack on key data holders by encrypting their files, with an intent to acquire sensitive data.

(e) Virus attack on navigation systems of ships to achieve chaos in fire accuracy of missiles.

(f) Malware attacks on aircraft avionics and drone guidance systems resulting in destruction of platforms.

As evident from above, the results achieved through CW can be devastating. Another aspect that needs to be understood is the entry of the attack vector into the Cyber domain. For this it is imperative to understand that in the Digitised TBA of future, the interflow of information in a networked system is divided into 'layers'. While each layer basically operates autonomously of the other, it is important to ensure that the data being transmitted from the host to destination has not been tampered with or is not being prevented from reaching its destination. The basic principles of Confidentiality, Integrity and Availability must be maintained and this is done using the four layered Transmission Control Protocol/Internet Protocol (TCP/IP) model. Some of the technologies for CW in these four layers are given hereafter.

**The Media Layer** refers to the erstwhile Physical layer and the new Ethernet layer of the Internet model. The vulnerabilities which can occur in this layer include Loss of Power, Loss of Environmental Control, Physical Theft of Data and Hardware, Physical Damage or Destruction of Data and Hardware, Unauthorized changes to the functional environment (data connections, removable media, and adding/removing resources), Disconnection of Physical Data Links, Undetectable Interception of Data, Keystroke & Other Input Logging.

A major security concern at this layer is tapping of the physical...
medium, be it Wireless or Optical Fibre or any other network cable. This allows an attacker to copy or even corrupt the data stream. The Physical Layer could suggest some type of physical action, like causing a denial of service by disrupting a power source, changing of interface pins, or the cutting of cables. The security issues become more pronounced when the network is based on a wireless media. A comparatively powerful transmission at same frequency can easily affect the quality of service; if not fully deny the service to the user. The chances of passive attacks on wireless media are more as it is more susceptible to interception.

The Network Layer performs network routing functions, fragmentation and reassembly, and report delivery errors. Routers understand the Internet Protocol (IP) and base routing decisions on that information. Address Resolution Protocol (ARP) in IPv4 or Neighbour Discovery Protocol in IPv6, matches a Media Access Control (MAC) Address to an IP address, and Routers make forwarding decisions based on IP addresses. The following are the key technologies used in Network Layer 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.** Routing Information Protocol (RIP) is used to distribute routing information within networks, such as shortest-paths, and advertising routes out from the local network. RIP has no built in authentication, and the information provided in a RIP packet is often used without verifying it. An attacker could forge a 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.** ARP is used to map IP addressing to MAC addresses in a local area network segment where hosts of the same subnet reside. ARP attack happens when someone is trying to change the ARP table of MAC and IP addresses information without authorization. By doing so, hackers can spoof his/her MAC or IP address to launch either Denial of Service or Man-In-The-Middle attacks.

(h) **DHCP Starvation.** A Dynamic Host Control Protocol (DHCP) starvation attack works by broadcasting DHCP requests with spoofed MAC addresses. This is a simple resource starvation attack just like a SYN flood. The network attacker can then set up a rogue DHCP server on his or her system and respond to new DHCP requests from clients on the network.

**Transport Layer attacks** involve the computer systems' 65535 ports. These ports can be further broken down into three categories: well known, registered and dynamic. Many applications utilize well known TCP and User Datagram Ports (UDP) ports. An attacker will gather information about a system using TCP. There are many ways to infiltrate, deny services, or scan networks. In order to prevent any data tampering, security in this layer is provided by Hypertext Transfer Protocol Security (HTTPS), or Transport Layer Security (TLS) or Secure Socket Layer (SSL). The key security risks associated with transport layer are:-
(a) **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. This ability of removing a host from the network for at least 75 seconds can be used as a denial-of-service attack, or it can be used as a tool to implement other attacks, like IP Spoofing.

(b) **Man-in-the-Middle (MitM) Attacks.** SSL was supposed to mitigate the risk for web transactions by providing endpoint authentication and encryption. However the feasibility of mounting a MitM attack on the protocol was discovered by hackers wherein they could either relay or manipulate the data between two users.

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

    **The Application Layer** is the layer closest to the end user, which implies that both the application layer and the user interact directly with the software application. Similar to the physical layer, the open-ended nature of the Application Layer groups many threats together at its end of the stack.

(a) **Backdoor Attacks.** One of the prime threats at the Application Layer is poor security design of the basic function of an application. Some applications may insecurely handle sensitive information by placing it in publicly accessible files or encoding it in "hidden" areas which are trivially displayed, such as in the HTML code of a web form. Programs may have well-known backdoors or shortcuts that bypass otherwise secure controls and provide unauthorized access.

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

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

(d) **Access Attacks.** Applications often grant excessive access to resources, allowing unprivileged users excessive access or imposing
inadequate control to prevent the corruption or loss of data. Cross-site scripting (xss) attacks take advantage of such vulnerabilities and create exploits for the same in malware.

(e) **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.

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

**Electronic Warfare (EW)**

EW is *warfare in the domain of the Electromagnetic (EM) spectrum,* which spans from 300 Hz to 300 GHz. This is the frequency band which facilitates transmission of EM waves in the Earth's atmosphere and it is divided into various bands for different applications, viz. Radio and satellite communications, Radar, Light propagation, Infra-red, Laser etc. This EM spectrum is the battleground of EW.

EW is further sub-classified into three actions; Electronic Support Measures (ESM), Electronic Counter Measures (ECM) and Electronic Counter Counter Measures (ECCM). Some militaries prefer to use the term Electronic Defence and Electronic Attack.

ESM includes all measures to identify and locate the 'hostile' EM source and includes the sequence of search and scan, monitor, identify and location fixing using Direction Finding techniques. The advent of Digital Radio and high speed processors facilitates the search and scan cycle at almost 10 GHz per second. Thus even frequency hopping signals at several thousand hops per second are tracked using eye diagrams and waterfall models. Having classified a radio transmission as 'suspect', the next stage is to identify it's source. This transmission can either be a radar signals, broadband carrier or a single radio user. The trend today is to create composite receivers to handle multiple types of signals. The approximate bandwidth can be ascertained from the spread of the signal and consequently an estimate of the digital bit rate can also be ascertained. The real challenge lies thereafter, in case the transmission is encrypted, as it now involves the process of demodulation and decryption. However, the
ECM is the active element in EW and involves the jamming of the hostile EM signal by using a high power transmitter such that the jamming signal is received by the victim receiver and not the intended signal. This can either blank out the receiver or lead to 'imitative jamming' to create deception. It may be noted here that signals from satellite transmissions are received at a very low signal level at the earth station user and thus the same are also prone to jamming provided the jammer is within the receiving arc of the receiver antenna. This can have a devastating effect on satellite based communications, as also the navigation based weapon systems, including missiles.

The author also includes the use of a non-nuclear high powered microwave source to generate an **Electro-Magnetic Pulse (EMP)** in the category of ECM. 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 active ECM is in the **Laser** band, where the Laser provides a very high accuracy weapon. This can be used as a 'Laser Dazzler' to blind the soldier or to cause burns on him or it can be used to burn out the electronics as in EMP. Laser Cannons are already deployed on some US Navy ships and Boeing is pursuing the CHAMP (Counter-electronics High-powered Microwave Advanced Missile Project) program with the USAF, which is a cruise missile with an...
electromagnetic warhead. Though Boeing has declined to discuss the project in any detail, a video produced by the firm shows the missile disabling a bank of desktop computers. Much of the work on such weapons is secret, but there are unclassified weapons as well. For example, the US military has funded a Radio-Frequency Vehicle Stopper - a satellite dish sized weapon that can be mounted on top of a jeep that can be used to disable enemy vehicles at a distance. Simultaneously the Chinese already boast of an airborne EMP capability and their Institute of Optics has recently developed an XRay pulsar which can cause devastating effects.

Finally, the aspect of ECCM in EW involves two parts, Anti-jamming measures and Anti-deception measures. Anti-jamming measures include the usage of chaff and decoys to mislead the jamming signal away from the target platform, and also the employment of spread- spectrum techniques to operate below the noise levels or the use of high speed frequency hopping signals which tend to evade detection. However, except for EMP hardening of electronic equipment, no other evasive measure has as yet been developed against the EMP weapons.

**Cyber Electronic Warfare**

Having examined the methodologies of CW and EW, we are now poised to understand the new concept of Cyber Electronic Warfare (CEW), which can be defined as the conduct of CW on an adversary using *the techniques of EW for ingress or incapacitation*.

Operations pertaining to EMP were hither-to-fore being classified under the nomenclature of Electro Magnetic Spectrum Operations (EMSO). However the author strongly feels that rather than have too many verticals related to individual weapon capabilities, it is time for a convergence of all related technologies in a particular domain, and hence we can merge EMSO in EW by considering it to be an extreme form of jamming that even incapacitates the electronic components and circuits. Similarly in CW, it was always related with soft attacks, however it can now be utilised to cause physical destruction also. A new deadly form of warfare is now created with the convergence of CW and EW. This form of warfare can be either Passive or Active. Passive CEW implies that a malware is inserted into the target network to cause soft attacks whereas Active CEW is the extreme form which includes the conduct of Jamming to deny the effective use of EM spectrum (and thus the network), to the enemy or the use of EMP weapons.
to destroy the electronics of the selected hostile platform.

In order to conduct cyber attacks through wireless networks, it is imperative to initially conduct EW operations to ascertain the network media characteristics. Subsequently, the choice is now available to the commander to either 'inject' a malware or to deny the service. Since this process is part of the same operation in the time continuum, it must form part of the same domain of warfare, and internationally the trend is towards convergence so that all the overlapping techniques are combined into a single integrated architecture. As an example, the F-35 fighter aircraft can perform reconnaissance, offensive/defensive jamming, and cyber attacks all from a single combat platform, thanks to the ability of its core processor to integrate diverse functions. If this be the model of future combat platforms, then there is no other option except to consider the converged CEW as an inescapable requirement of the future battlefield.

Conclusion

The future tactical battlefield will be replete with wireless networks providing the media for battlefield management systems in the informationised combat environment. The logic of a more integrated approach to cyber and electronic warfare is not just functional or operational -- it is also financial, and would lead to rationalisation and budgetary optimisation in defence procurements. In a recent article, the Chief of US Naval Operations has argued that cyber weapons needed to be merged with electromagnetic attacks, or what he calls the "electromagnetic cyber realm." He goes on to say that "The EM-cyber environment is now so fundamental to military operations and so critical to our national interests that we must start treating it as a warfighting domain on par with-or perhaps even more important than-land, sea, air, and space...Future wars will not be won simply by effectively using the EM spectrum and cyberspace; they will be won within the EM-cyber domain."

In this article, the author has combined the existing methodologies of CW and EW, and propagated the converged concept of Cyber Electronic Warfare (CEW). It is imperative that the same specialists be now trained on both these techniques so that this domain of future wars can be fully exploited and commanders are presented with a battle winning option, both for offensive and defensive operations. In the emerging era of Non-nuclear Non-kinetic warfare, CEW presents to the commander the
Mother-of-all-Non-kinetic Threats.

Lt Gen Rajesh Pant is an internationally renowned Techno-Scholar-Warrior-Mentor. He is presently the Chairman of Precision Electronics Ltd and a Governing Council member of IETE New Delhi.