CYBER-SPACE: IMPLICATIONS FOR NATIONAL SECURITY

A.K. TIWARY

Nothing Remains, Neither the State nor Wealth nor Valour without the Security provided by the Armed Forces.

— S H Ukraniti

CYBER SECURITY

Cyber space and the possibility of cyber war, as it emerged in the late 1980s got mixed up with Information War (IW)/Electronic War (EW). This led to numerous definitions of IW/EW/cyber war, and most definitions, instead of clarifying the issue, only created further confusion. For the purpose of this paper, the latest definition of cyber space, promulgated in the USA in 2010 being the most comprehensive, has been adopted. It defines cyber space as, "A global domain within the information environment consisting of the inter–dependent network of information technology infrastructure and resident data, including the Internet, tele-communication networks, computer systems and embedded processors and controllers."[1] This indicates that there is a physical domain of hardware, and an information domain of software. How we deal with the information or data resident in this domain to deceive the enemy/cyber criminal becomes part of the third domain—the cognitive domain. As the paper analyses the hardware and

A.K. Tiwary

1. Martin C. Libicki, "Cyber Deterrence and Cyber War." Rand Project Air Force, Santa Monica, CA, 2009.p.13.

XXX

software domains to discern their vulnerabilities, one must keep in mind the cognitive domain and the attendant possibilities of solutions to the problems that seem insurmountable in the earlier two domains.

When we talk of cyber security, we mean security of each component in the above definition as well as successful performance of the system as a whole, more so when under attack. To understand the type and amount of threat to cyber security and its resultant impact, let us briefly look at the attackers/ criminals in the cyber space and their modus operandi. The attackers/ criminals could be classified into individuals, small groups of individuals, criminal gangs, terrorist organisations, patriotic groups and, finally, the proper cyber organisation at the state level, created and maintained by the state. The threat could be financial fraud, data theft, espionage at the corporate/national level, and damage to software and/or hardware, which could also result in physical damage to systems/infrastructures run by the computer network. The targets could be civil as well as military.

Individuals: At this level, individuals deal mostly in financial fraud, credit card data theft**,** siphoning money from bank accounts, stealing passwords, stealing data to sell **or** misuse. Some eccentric individuals also invade cyber space for strange reasons. One such case was of a Taiwanese computer engineering student named Chen Ing Hau.He created, "Chernobyl or Win-CH" virus which damaged thousands of computers on 26 April 26, 1999. The stated purpose of the creation of VIRUS was to humiliate incompetent anti-VIRUS software providers! Thereafter, he lent a helping hand in fire-fighting his own VIRUS.[2]

Terrorists: Unlike any other medium, the cyber medium is easiest to access and communicate/intrude with others worldwide, often undetected. Attribution as to who and where the attack originated is difficult to pinpoint. Therefore, terrorists prefer to use cyber space to their advantage and also

2. *The Times of India*, January 29, 2000.

to create havoc and fear among the public to gain propaganda mileage. **XXX**

Criminal Gangs: Operating within the deep web, where anonymity is ensured,criminals are offering drugs, criminal services including assassins for hire. One such gang called Silk Road was unearthed by the Federal Bureau of Investigation FBI in September 2013.[3]

Patriotic Hackers: These voluntary individuals, either individually or in collaboration, express their patriotic sentiments by attacking known/perceived adversaries. This often happens between India and Pakistan. In China, it assumed massive proportion after the US attack on the Chinese Embassy in Bosnia in 1999 and after a mid air collision between a US spy plane, a P-3C Orion, and the Chinese fighter interceptor in which the Chinese pilot suffered fatal injuries. The Chinese government overlooks such hacking activities. At times, it supports it for national purposes. It even recruits from amongst such hackers for a Chinese web militia. It is believed that the civil web militia planned by Chinese numbers many thousands of hacktivists. Mostsuch hackers remain nonpaid recruits.[4]

Corporate Espionage: Some Corporates, at intra-national as well as international level indulge in cyber espionage to steal technical data, consumer behaviour data, etc. and to find the strategies of competing corporate houses. As the volume of data keeps increasing towards the infinite, its analysis helps a lot in furthering marketing and designing of newer products. This activity could also be backed by the state. It is alleged by the USA that the Chinese government as well as Chinese state companies have been stealing data from US companies to catch up with new complex technologies. Richard A. Clarke, a cyber adviser to US presidents from 2000-2010 reinforces the above allegation. Among many technologies stolen, extensive software data of the F-35 fighter plane, - the latest US fighter is also alleged. A cursory look

3. *Time*, October 21, 2013, p.15.
4. *The Times*, April 15, 2013. pp.40-42.

at the remarkable rapid development of Chinese military aviation seems to reinforce the US claim.

State Level: Cyber activities by a state should be considered at two levels. One is the cyber attack as a preliminary integrated step of an active war. The targets are not only military but could also include critical infrastructure like the telecom network, power distribution, power generation, financial services, media, etc..,Some known examples are the Israeli cyber attack on the Syrian air defence network in 2007 when Israeli warplanes struck at Syrian nuclear sites. In 2010 Iran's nuclear enrichment plant's centrifuges were attacked using the Stuxnet VIRUS which impacted the control mechanism and caused thousands of centrifuges to overspeed and self-destruct. Estonian networks were attacked(distributed denial of service) in 2007 and made non-functional for a few days as a reaction to removing an earlier era Russian war memorial from Tallinn, the capital, to a cemetery. Georgia was cyber attacked along with conventional Russian attack in 2008. The other level is cyber espionage during peace-time. For such ventures to be successful, a whole lot of exploratory work, cyber preparation, development of specific cyber weapons, etc. needs to be undertaken. Cyber defence and offence are continuing cycles. As a threat develops and is detected, counters are developed to nullify the threat. These are called anti-VIRUS programmes or security patches. Whereas, a conventional bomb or a missile once produced remains a threat forever, this is not so for cyber weapons. In the cyber world one has to keep designing new weapons as old ones become negated quite fast. Even pure cyber defence makes it essential to develop cyber policing tools. Perforce, these are offensive in nature and design.This blurs the traditional difference between defence and offence in cyber space.

Cyber Weapons: Having seen the cyber actors,one needs to have a look at cyber weapons and their classification. This is essential to understand subsequent actions by the cyber warriors as also by the strategy makers. Basically, there are two types of cyber weapons, the SIGNATURE type and the BEHAVIOUR type. VIRUSes and WORMS are the signature type as they have their distinct signature. Thus, they can be recognised by filters, firewalls, anti-virus programmes, etc.. Behaviour type weapons are

extremely difficult to detect. The above devices cannot detect their presence. They may remain undetected for months engaged in their unauthorised activity. The counters can only be made once their presence is detected. This makecyber activities highly complex, demanding numerous experts in multiple cyber disciplines. Starting from a small beginning in the 1980s, today the USCYBERCOM employs around 27,000 personnel in the cyber field and plans to urgently train "cyber warrior" specialists numbering 6,000.[5]

VIRUS: The initial cyber attacks were characterised by a VIRUS programme entering the computer. A VIRUS is an undesirable software programme that causes damage to information within the computer. Its full form is "Virtual Information Under Seize". This software attaches itself to either a programme or a file. It can infect software and /or hardware. It can be mild or severe. A human action is required for the VIRUS to enter. The most common human action is to open an infected link. Unfortunately, there is no way of making out an infected link from a normal link.Both appear the same. Since 1989, when the first VIRUS was made as a deliberate experiment, today, there are more than one million VIRUSES. Their number doubles every 8 ½ months. Once a VIRUS is identified, its anti-VIRUS programme is made to nullify the VIRUS. So the anti-VIRUS is a reaction strategy. It is not preventive. A certain amount of damage will take place till the anti-VIRUS is made and implemented.

Worms: These are VIRUSES which travel/infect computers by themselves. No human action is required like clicking on a link or opening an attachment. They also replicate themselves, thereby saturating the affected computer or server. They can damage the affected system immediately or plant unwanted cyber weapons like the Trojan horse, Scanners, Sniffers, Logic bombs, etc..

Behaviour Type Cyber Weapons: VIRUSES and WORMS are recognised by their signature, permitting detection, and creation of anti-VIRUS software. The other cyber tools like the Trojan horse, Botnots, blended programmes, spear phishing, mutating/ polymorphic VIRUS, scanners, sniffers, etc. do

5. Ibid., Libicki.

not have a detectable signature. They enter a computer piggy back on a friendly permitted programme. So security systems treat them as friendly programmes. Once inside the system and activated, their actions leads to abnormal behaviour. It could be vast damage/destruction of software; takeover of affected Personal Computers (PCs) and servers; stealing of data, etc.Their detection requires constant monitoring of the system behaviour. Any abnormal behaviour monitored is to be investigated. This makes their detection extremely difficult because it is not so straightforward to classify system behaviour into normal and abnormal, more so as the system complexity itself increases. ATrojan horse can create a backdoor entry into the affected computer or server. Botnots permits remote control over computers, even from halfway around the world. Spear phishing is insertion of remote access tools. Polymorphic VIRUSES mutate themselves, thus, assume new signatures which the anti-VIRUS cannot detect. Scanners detect security holes in the hardware/software. Sniffers record information. Trace routers trace the network route. Password crackers decode passwords. Logic bombs trigger an action which could cause software/physical damage. The two famous examples are the Stuxnet attack on Iranian nuclear centrifuges which overspeeded thousands of centrifuges resulting in their destruction. Other was the causing overspeeding of a Russian oil pipe line motor, which resulted in the pipeline explosion and a massive fire. Both are believed to be handiwork of the USA.

Zero-Day Vulnerability: When new software and hardware systems are developed, they are initially run over a period of time to try out the system; to find the weaknesses and their rectification. This is called the beta version. After the beta version, the new systems are marketed. Yet in this complex cyber world, – the new systems have weaknesses not yet noticed by the manufacturer in spite of trials during the beta version. But the same weaknesses are uncovered by hackers. The period between introduction of a new system and rectification of weaknesses discovered by hackers is called zero day vulnerability. During this period, there is no defence against cyber attacks. This period could last long if the hackers do not divulge the weaknesses, and plan to use then for nefarious purposes. Or even after the

weaknesses have been brought to the manufacturer notice, the manufacturer himself may take time to design the proper counter.

Zero-DateVulnerability: Even after designing the security patch for zero day vulnerability, some time elapses till the patch is installed on the affected systems. There will be many persons/organisations who are not aware of the new security patch or are lazy in its procurement and installation. Of course, a pirated operating system cannot be patched up. So the affected system remains vulnerable. This period is termed the zero-date vulnerability period.

Detection of Cyber Attack: A VIRUS or malicious software called 'malware' needs to be detected to keep a computer safe. The first line of defence is a firewall. It is a software/ hardware or combination that checks each new data packet wanting to enter a computer. Based on certain rules and logic, it does not allow unwanted data packets to enter. The next line of defence is by way of an intrusion detection system looking for unauthorised entry. Thereafter, the defence is by the "anomaly detector."

Anomaly Detection: A network/system/computer has software which manages systems information and events within called SIEM (System Information and Event Management). It is a sort of watch dog over all the activities taking place. It watches firewalls, authentication process, authorisation levels, access rights to various users, working of switches, routers, servers, content filters, data storage, data usage, analyses, etc.. It compares the multitude of activities with what is permitted in programme and detects anomalies or abnormal behaviour. For instance, if a low level user accesses information allowed only to a high level user, this will be detected as an anomoloy and investigated. Since cyber attacks without a signature trail as in a Trojan horse give no indication of entry into the system, it is only the subsequent behaviour of the computer, like stealing large data/unauthorised entry/unauthorised extraction of data, etc.or any other abnormal behaviour which will give the first indications of malicious activities.These types of attacks have become more common in the last decade and are known as "Advanced PersistentThreat (APT)". The system can be under attack for months or even years if the malicious software

XXX is being run with great care. The Chinese are believed to have done extremely well when they penetrated many systems in the USA and stole massive amounts of data from the defence and aviation industry.

SIEMs designing is complex and needs dynamism. If there are too many false positives, it reduces the system's operating efficiency. It will slow down the system excessively defeating the very purpose of the security in the first place. If there are too many false negatives, then the security provided will be inadequate. What is normal and what is abnormal behaviour is not easy to define – making detection difficult. The process is an ongoing one requiring corrections and tweaking often. It needs constant interaction between the users of the system and the security providers. An organisation requires many specialists, multiple cyber tools, cyber experience and enormous patience to deal with APT. That is why the cyber defence is for more expensive than cyber offence.

RECOMMENDED STRATEGY FOR CYBER SPACE SECURITY.

Press reports indicate that a lot of work has been done for cyber security in India. Since public knowledge is limited and an outsider is not aware of the current status of the cyber security programme, one can only list down what should be done theoretically. The following recommendations are based mostly on a study of US efforts, especially of the US Air Force (USAF) as it is the lead agency for cyber space. Also, the USA can be considered the motherland of the cyber world. The first chip was made in the USA. TheInternet was born in the USA and is even today owned by the USA. The world uses the Internet free kind courtesy the US Department Of Defence (DoD). Microsoft and Silicon Valley have led the software/ hardware development. The USA has maximum experience in the cyber world. Its cyber journey since the late 1980s can be summarised as follows. The USAF recognised the possibilities of cyber warfare early on.It

XXX

experimented within, with the industry, and with the academia for cyber knowledge and cyber experience.Its cyber organisation, started with an IW cell in the 1980s; an IW Centre established at Kelly Air Force Base in 1993 has now grown into a Cyber Command (CYBERCOM) ,achieving Full Operational Capability in 2010. The USAF CYBERCOM is part of the US CYBERCOM. A 4-star General, Keith Alexander, heads the US CYBERCOM. He also heads the infamous National Security Agency (NSA); and is responsible for cyber support to Department of Homeland Security (DHS), and the central security services. The US CYBERCOM partners with 100 universities for cyber education and recruits from amongst their graduates. The NSA itself has 700 PhD professionals and the rest of the cyber force benefits from their technical expertise. The NSA has invested huge amounts of money in super computers and data storage, data analytics, etc.. The USAF has a manning of 15,000 in the USAF CYBERCOM.A new cadre, Cyber Warrior, has been established, with rigorous cyber training and testing, incentive pay, career progression, etc.. It conducts many exercises including participation in the "Red Flag" Exercises.

Apart from the USA, not much in known about other countries' cyber set-up with certainty. Israel is believed to have invested heavily in cyber capabilities. China is also believed to be in cyber space very seriously. But all the countries are behind the USA in cyber experience.We are also aware that the USAF model has evolved, being put to test regularly in wars since the Iraq War 1991, Bosnia in 1995, Kosovo in 1999,Afghanisatn in 2001and Iraq in 2003. So it is a product of war-time experience. Therefore, it is a good model to study and adapt with modifications, as necessary, for our conditions. A brief account of the USAF cyber organisation and its experiences follows.

The USAF set up IW Squadrons in the 1980s. As a result of the success of IW in the Gulf War 1991, the USAF decided on IW across the full spectrum of command and control. So the 688th Information Operations Wing was set up. The wing has technical skill sets of the AF Electronic Warfare Centre; and the AF Cryptographic Support Centre's Securities Directorate, and intelligence capabilities from the former AF Intelligence Command.

In 1993, the USAF established an IW Centre at Kelly Air Force Base, Texas. By the mid-1990s, the IW flights, consisting of 25 personnel each, would work alongside the CAOC (Combined Air Operation Centre) whenever operations were going on. IW operations were undertaken during the Bosnia operation in 1995 and against Serbia in 1999. The comprehensive operations included EW against radars and Surface-to-Air Missiles (SAMs), cyber attacks against Integrated Air Defence System (IADS), operations against televisionand Radio, as well as cyber attacks against computer based systems like power generation, oil refining systems, etc..

In the past, the USA caused a massive explosion in a new trans-Siberian oil pipeline running from the Urengoi gas fields in Siberia across Kazakhstan, Russia and Eastern Europe. This was done by causing its pumping station to overrev by computer malware, in cooperation with some outraged Canadians, who had supplied the software for the pumps.[6] The US navy (USN) established its cyber cell in 1999 and mandated the unit to become like the 'Top Gun' amongst fliers.In December 1998, the DoD / USAF established the Joint Task Force on Computer Network Defense (JTF – CND). It was headed by a major general and was to work with the US Army, Navy and Marine Corps. This was an immediate result of a massive malware attack on US military nets. It took the US 14 months to clean up this virus, termed Solar Sunrise, from its systems, numbering more than 500. It also revealed the enormity of possible damage to improperly secure networks.

Cyber War exercises named "Eligible Receiver' and "Solar Sunrise' were conducted in which federal agencies / Services, Israeli analysts and

6. Thomas C. Reed, *At the Abyss: An Insider's History of the Cold War*, (New York: Ballantine Books, 2004), p. 268

Californian teens attacked defence networks. Weaknesses and vulnerabilities were identified and preventive steps initiated. In September 2001, the Pentagon created Joint Task Force- Computer Network Operations- (JTF-CNO). The Computer Network Operations (CNO) replacing CND implied a need to attack in order to defend proactively. From defence to offence was a major change in strategy.

Cyber defence now meant the following: secure all exclusive networks in which individuals cannot plug in pen drives, CDs and external devices. Ensure defence in depth by installing firewalls. When under a cyber attack, the system should degrade gradually rather than have a catastrophic collapse. When the attack is over, the system should recover.The system should be self-diagnosing and have built in healing capability.[7] Data bases must employ stealth methodologies where, for example, modulating chip technology enables then to hide, morph and masquerade as effectively as any attacking agent. Also, cyber security relates to place and time. Unlike conventional war, in which offense is the best defence, in cyber war defense becomes primary because of nature of attacker. There are no hostile cyber bases which preemptive cyber bombing can destroy. The recovery from an attack can be fast. The success of the cyber-attack itself cannot be known with certainty.

In 2001 USAF placed Cyber Wing under Space Command. By May 2002 it had a manning of 340 personnel. Later Cyber Command was made a sub unit of US Strategic command. Cyber command looks after all military networks numbering 15000 in all the Services. It has replaced the earlier Joint Task Force – Computer Network Operating and the Joint Functional Component Command for Network Warfare JFCC – NW. It has under it the Cyber Commands of US Army, Navy, Marine Corps and Air Force. It is responsible for both defense and offense in Cyber War. In addition it provides technical and electronic warfare support to Department of Homeland Security (DHS). If and when asked by DHS it will provide additional assistance. DHS looks after civil and private networks. NSA

7. "USAF Strategy – Past, Present & Future 2018 – 2023" AF Research Institute, 2008 Gen John A. Shaud Ph. D Air University, January 2009.pp. 45 – 50.

looks after all the government networks apart from the ones in military domain. USCYBERCOM has been tasked to develop:

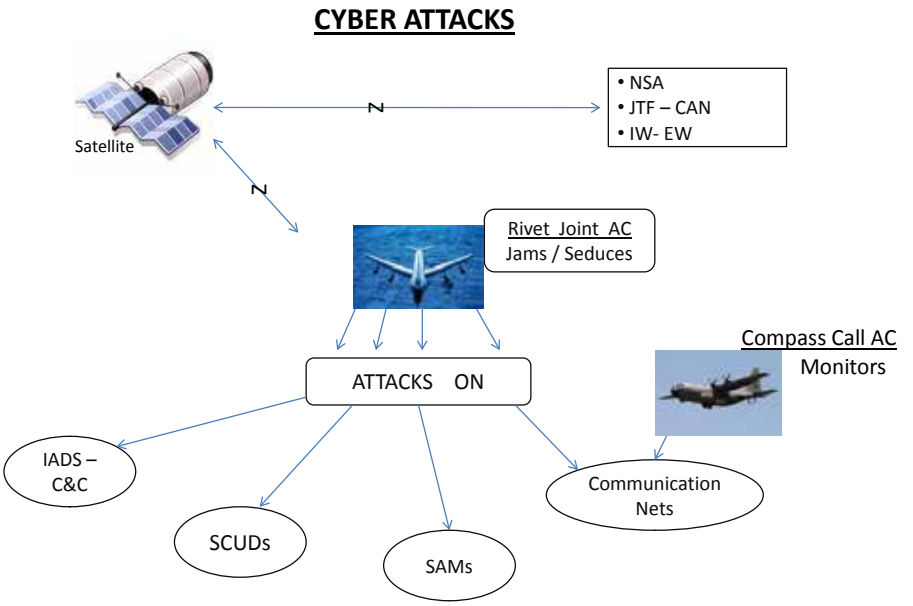
- Methods to assess operational impact of intrusions.
- Identify proper response.
- Co-ordinate action with appropriate organizations.
- Prepare Response Plans.
- Execute plans through Service components.

US CYBERCOM will also issue Operational Alert conditions depending upon detected threats. The conditions are normal, A, B, C& D. Over and above these arrangements the Cyber organizations seeksupport and rely on private security specialists companies to deal with cyber threat.The earlier concept of cyber security was purely defensive. However, as the cyber process and attacks kept increasing, especially post 9/11 and after the incident of US spy plane P3C Orion's collision with a Chinese interceptor in which the Chinese pilot died, USA selected a new strategy for cyber security. This was a result of sustained persistent attacks on their networks. In 2006 a new term was coined- Advanced Persistent Threat (APT). Such a long duration attack could be a result of attacks by another state or by organised criminal gangs who steal data in order to sell it. The method adopted was in three phases. Initially the attacks were to recce, launch and infect the targeted network. After identifying vulnerabilities, the target was infected. In the next phase, control of the network/machine was taken over, attacks were updated, data was discovered and exfiltration persisted till it was stopped by the host. The attack would also be spread to other machines.Against APT, it was felt that a purely defensive strategy was reactive and insufficient to ward off theb cyber threat. There was a need to monitor the content and context of outgoing data, and links visited. The web gateways needed to be secured. There was a need to monitor incoming data as well as e-mails and data across the web. For proper cyber security, there was a need to actively patrol the cyber network for detecting potential trouble. Since the original Internet IPv 4 has many security weaknesses, it was necessary to develop a new Internet. The new Internet is called IPv

6.To reduce vulnerabilities, the external access point of the GIG (Global Information Grid) was reduced from 120 to only 16. All 8,50,000 users were integrated into one common GIG/AFNET which was provided embedded security. Thus, the defence was made stronger and now the attacker was forced to work harder to find vulnerabilities.

Rivet Joint is an specialist transport aircraft (KC-135) which is used for CNA. It is in contact with agencies like the NSA, JTF – CNA, and IW–EW centres via satellite links to receive and send back the latest information for CNA planning. It injects cyber weapons, as appropriate into the hostile IADS network, the Scud type missiles command and control centre and the communication networks. Another special aircraft called Compass Call (C-130 modified) monitors the effectiveness of communication networks.

Fig 1: Cyber Attacks



In the USA, the 24th AF looks after cyber operations.Manned by 14,000

airmen, the 24th AF has three major wings and an operations centre under it. These are:

- **67th Network Warfare Wing:** It looks after information operations. Its 8,000 strong manpower is located at some 100 locations worldwide. There are 35 squadrons and these deal in the operations of television, radio, telephone exchange and networks including mobile phones and networks.
- **688th Information Operation Wing:** This deals in cyber space Research and Development (R&D) and is manned by 1,000 staff members who are a mix of the military and civil.
- **689th Combat Communication Wing:** Its mission is to train, deploy and deliver expeditionary and specialised communication; and air traffic and landing systems for relief and combat operations.

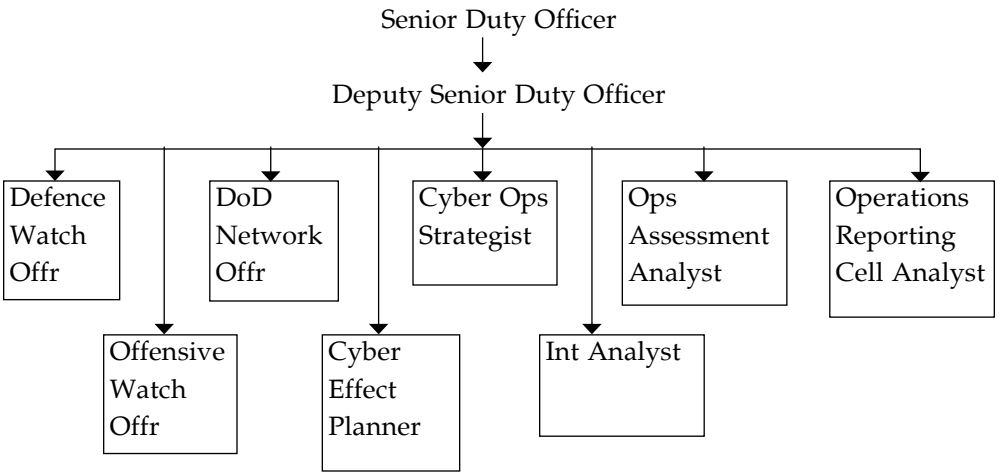
USAF leadership has adopted a novel approach, to overcome bureaucratic procedures and fast track cyber development. For the Iraq War, 1991, they had created a Combined Air Operation Centre (CAOC) in Saudi Arabia on an ad hoc basis. The CAOC turned out to be a phenomenal enabler for successful prosecution of the war. But this ad hoc arrangement hindered proper establishment of CAOCs in other commands subsequently. Therefore, in 1995, the USAF declared CAOC to be a weapon system essential for war fighting. They named it the Falconer Weapon System. This allowed proper authorisation, financial allocation, manpower, training, standardisation, regular testing, etc.. A similar approach has been adopted for CYBERCOM. The USAF has established six cyber weapon systems. These are:

- Air Force Cyber Space Defence Weapon System.
- Cyber Space Defence Analysis Weapon System.
- Cyber Space Vulnerability Assessment Hunter Weapon System.
- Air Force Intranet Control Weapon System.
- Air Force Cyber Security and Control System.
- Cyber Command and Control Mission System Weapon System.

A first look at the above list may indicate duplication of work. This is correct, but is needed. To illustrate, all SAMs are meant to shoot enemy

aircraft, yet we have the short range SAMs, medium range SAMs and long range SAMs. Similarly, all transport aircraft are meant to move men and cargo from one place to another. Yet we have the C-17Globemaster, C-130 Hercules and yet smaller transporters. Therefore, the arrangement in cyber space is similar. Without going into the tasks of each weapon system, the set up of only one weapon system is illustrated below (Fig 2) to show the multifaceted nature of work in cyber space.

Fig 2: Cyber Command and Control Mission System



China's rapid rise has compelled the USA to enter into a strategic partnership with India. We must capitalise on this opportunity. In the cyber field, the US has agreed to provide courses in cyber security, critical infrastructure protection, financial terrorism and anti-terrorism intelligence. In addition, the US will help in creating specialised training institutions to develop skills, capacity building and technology development. All the concerned departments under the Ministry of Home Affairs (MHA), nearly 15 of them, send their personnel to the USA for training. The training modules include cyber security, cyber forensics, technical surveillance counter-measures, control systems security programme for end to end networks and system security for servers, routers, switches, transmission and all

XXX Information and Communication Technology (ICT) hubs and facilities including encryption/ decryption.But as we do this collaboration with the USA, we must not forget the shenanigan of the NSA, and take all the necessary steps. As per a reputed report:

- The NSA has deliberately introduced flaws in many encryption systems on the Internet in order to weaken them for the NSA's intelligence collection.
- Software companies and Internet Service Providers (ISP) were asked to insert secret vulnerabilities and backdoors into apparently secure systems.
- The NSA has set lower encryption standards for the industry, which it is able to break into.
- "Five Eyes "i.e. the USA, UK, Australia, New-Zealand and Canada tap into fibre optic cables to steal data.

The cyber world is connected by communication nets. So a brief look at communication security is in order when we talk of cyber security. Edward Snowden's wikileaks about the US NSA eavesdropping on friends and foes alike have once again brought communication security into prominence. We need to remember that this has been an ongoing programme carried out by the USA—earlier, under the nomenclature of Project "Echelon" since the 1980s, and now the same, though greatly upgraded, it is called Prism and Muscular.The current Standard Operating Procedures (SOPs) for telecom security are good enough provided these are followed religiously. In addition, at the strategic level, we need to again review communications with the following in mind: separate the one way communication from two-ways communication. A large portion under one-way can be unclassified like weather information, welfare information, etc.,Separate real time information from the rest. For example, warning of an air attack/missile attack/rocket attack may not need classification because it is of no interest the moment the

XXX

event is over. Plan encryption level commensurate with security classification. Cryptography must be developed indigenously. In this we should be wary of encryptions standards set by the USA (NSA) internationally—Edward Snowden has revealed the, NSAs blatant interference.Plan to integrate radio, TV, Twitter,Facebook, and U-tube for passage of warning or relevant information. These means could be either primary or as back-up, depending upon various activities.Plan to use commercial satellite channels – Indian as well as international. Also plan to use transponders in all bands like C, S, Ka, and Ku. It will be very difficult to jam all the above.We have 250 plus languages and dialects. Use them as natural encrypted communication, at least as back-up.Fibre optic cables are mostly underground/underwater. Their physical security becomes more important in the light of the revelations about Western countries tapping in to the fiber optic cables of companies like Google, Yahoo, etc. for data. Unmanned Aerial Vehicle (UAV) communication links and the aeronautical telecom networks are all open and use the Internet. The Internet IPv4 has many security holes due to its evolution in the civil field. UAV frequencies are open, unregulated and manufacturer- specific. There is no mechanism for authentication and encryption. Sequence number spoofing, and authentication attacks are possible. Denial of Service, (DoS) TCP 'SYN' attacks during 3-way handshakes are also a reality. ICMP/ CMP attacks are unreachable.To remedy the problems listed above, the following are suggested. Use AES encryption algorithm on unsecured links. Use authentication for UAV control. Use mobile Internet Protocol (IP) technology for UAV address. Use the "make before break" strategy for UAV handover. Specify that UAV software upgrade to be done only on the ground.Consider firewalls, shielding, SNMP version-3, and anti-jamming circuits for UAVs. Reduce electro-magnetic interference caused largely by own IED jammers unintentionally jamming our UAVs.

CONCLUSION

While the cyber threat is real and serious, it is certainly not like another dimension of war as in the land, on the sea, and in the air. It is more akin to EW which complements and enhances conventional attacks. Cyber attacks can create corridors through which other attackers can attack more effectively. It may also lead to physical damage. But the consequences of cyber-attacks can be controlled before too much or catastrophic damage is done. Cyber espionage, on other hand, can cause far more loss by enhancing attacker's capability, provided they have the means and the will to exploit the stolen data. Therefore, a proper balance of defence and offence is essential for cyber security.