Thirteenth Colonel Pyara Lal Memorial Lecture Cyber Warfare and its Implications for National Security

Mr KVSS Prasad Rao**

Ladies and Gentlemen, it is my privilege to be amongst you today to share some thoughts and exchange views on this relatively new 'Tool of War' that has entered the lexicon. This lecture, you are all aware, is in memory of Late Colonel Pyara Lal who served this fine institution for 30 years from 1957 to 1987 and died in harness. He rendered yeomen service to USI and the library here is named after him as our token of remembrance and gratitude.

Cyber War is supposed to be a new dimension, a new arena. Many of us must have seen numerous Hollywood movies, in which we see lots of things like bringing down dams, shutting down power plants, crippling industry and even diverting and disarming of enemy's nuclear missiles in their flight, just by a click of a mouse. What is hype and what is real? Where and how is this particular warfare waged and what it would mean to our security? Some of these are issues that I would like to touch upon in this distinguished gathering today.

Cyber Space is a term that seems to have been first used by William Gibson in one of his Sci-Fi novels. Many believe that it will be the fifth dimension to land, sea, air and space as a theatre for war, and conflict. This is a man-made construct and there is no concept of physical distances or boundaries here. It changes its configuration, its structure, both micro and macro, with time so often that it is neither consistent nor deterministic. If you, for instance, use Cyber Space to send your command or message you can never predetermine at what time it arrives and what route it takes. It may take different routes and arrive at different times.

If you take Cyber Space as an arena for war, we need to have certain clarity in terms of how it is defined and managed in different ways. But if you go through the available literature and records, there is no clear agreed definition even to this day. William Gibson, whom I had mentioned earlier, had defined it as "a shared virtual environment whose inhabitants, objects and spaces comprise data that is visualised, heard and even touched" but then, this is very abstract and conceptual. But most commonly, you would imagine the internet as a World Wide Web – an information sharing environment between computers - this is what everybody commonly thinks of as Cyber Space.

If we look at the US Joint Doctrine, this word is defined as "the notional environment in which digital information is communicated over networks." On the other hand, the US National military strategy for Cyber Space operations document is more specific and somewhat more different in their approach i.e. "...defined as a domain characterised by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructure". It is interesting to observe that as per joint National Military Strategy the entire electromagnetic spectrum also forms part of Cyber Space and also in their view, includes exchange networks like Tactical Digital Information Links (TADIL) between command and control platforms and air, ground and sea weapon systems where some kind of network data links are present. While opinions on the gamut of cyber space may vary, it is important to remember at this stage that it definitely includes some of our critical infrastructure – that part which relies on or is connected to the information infrastructure.

When we begin to consider Cyber Space as a war arena, being a man made construct, it has all the frailties and fickleness of our own creations. We also need to consider the objectives of Cyber Warfare : What objectives would one like to realise, when we launch a cyber attack ?

Now coming to the question : Can Cyber Warfare or attack be a stand-alone activity or has it to be an integral part of a wider operation where other media are also involved like land, air etc ? In the military context, many experts feel that, for the present, it is more a force multiplier, than a force itself. But when it comes to economic warfare, the situation is very different. Then it can be strategic or tactical in its scope, nature and its effectiveness. If Cyber Warfare is considered as a 'War' then the standard norms, definitions and concepts of war should be applicable, such as deterrence. Can it be graded into a high intensity or low intensity conflict? Is the damage assessment on the enemy's assets possible ? After all, ultimately, when we talk of war, war itself has no meaning unless it inflicts some kind of unacceptable damage on the target.

How predictable are the efforts? Because of the randomness of the Cyber Space and its non-deterministic nature, the effects are not predictable as with other weapons. What kind of pre-conflict preparations does it call for? Every warfare calls for lots of planning and logistics et al. How do they manifest in Cyber Warfare? Can sustained strategic sabotage using Cyber attack be considered as an act of war? For instance, what kind of threshold is there to distinguish between an act of war and pranks, or Cyber crime? Is it repeatable in its effectiveness? After the first attack, the affected party may discover and close the vulnerability and afterwards that particular Cyber weapon could be useless.

Are there any rules of engagement? How do we control escalation? This is an important issue because if Cyber War is construed as a war in the kinetic sense then, the people who do not have the cyber capability to retaliate could resort to other forms of warfare including conventional warfare. Then, how do you control escalation? Are

there any international laws or conventions that control the Cyber Warfare? Not specifically. There is no Geneva Convention to control Cyber Warfare. There are also different views on this. Can it be limited to national boundaries and is the issue of sovereignty addressed? When it comes to Cyber Warfare, there are no physical boundaries. If an attack is launched from place X on to place Y, the attack could go through a number of other countries, not necessarily directly from territory of X to territory of Y. As a result, sovereignty issues crop up. Are you violating not just the laws of the target country, but also the laws of other neutral countries through whom you are routing your attack traffic?

Cyber weapons are basically software codes which can be spread across a network. They are most-commonly viruses - Worms, Spyware, Key loggers, Malware, Trojans, Bots and Botnets etc. Cyber weapons are very different from conventional ones and they are very easy to replicate. You can produce a number of copies without spending much money. Here, all your expenditure is in the creation of the first original. They are easy to disperse in large numbers, difficult to trace back. Since, traceability in this case is difficult and so is the deterrence.

Cyber weapons depend upon the targets' vulnerabilities. Cyber War is waged where there are vulnerabilities. If there are no vulnerabilities in the software and hardware of the target systems, you simply cannot break into cyber space. But fortunately or unfortunately, the systems are so complex, it is virtually impossible to have systems which are vulnerability free. As you evolve you correct one vulnerability and in the process you create some more. In addition, certain vulnerabilities are left there deliberately by the people who have the control over them for obvious purposes. Because of this, Cyber weapons are sensitive to time and space in the sense that if they work today, tomorrow these may not work because those flaws have been corrected. And whatever Cyber Weapon you have developed, it is ineffective once that particular flaw is closed. You now have to look for new flaws and new vulnerabilities. You all are aware that Cyber Space software is fast-changing and fast evolving. So your weapons and tools also have to evolve with equal speed and alacrity otherwise they become useless. Also, if you expose your knowledge of a vulnerability, you lose out on that vulnerability. You have to be very secretive. This is also very important.

Some time back mention was made about the critical infrastructure of a nation. If you see critical infrastructure like power, distribution networks, dams, power stations etc. for both economic reasons as well as for the purpose of convenience and efficiency, their operations are getting automated. A standard called Supervisory Control and Data Acquisition (SCADA) is the standard that is used in many of these infrastructure facilities to control their operations. Economics drives the need to make products cheaper and reliable so that customer is satisfied. These are the two most important factors as far as a customer is concerned. As a result, designers and manufacturers try to choose known, well established standards like Internet Protocol Standards, SCADA etc. The advantage is they are already developed. It makes tremendous sense for any utility to use systems based on such existing technologies to cut costs. Secondly, they have been tried and tested thoroughly, and as far as the reliability of operations is concerned, it is the best they can get. This is what drives the industry to go for these standard protocols and the standard practices. But from the purely security point of view, it has a disadvantage. The disadvantage is that they are known to everybody and many people discover vulnerabilities and develop techniques to exploit these vulnerabilities. So this is the negative side of going for this well known and established standard protocols and standards of software and hardware. That is the reason why, some of these systems are increasingly vulnerable to Cyber Warfare and cyber terrorism attacks.

What kinds of threats do you expect from Cyber Warfare?

(a) For an **intelligence gathering purpose,** a tool for cyber information gathering and espionage. This is much easier to use and with much more potential for damage, compared to any other type of espionage. What makes it different from others is that you achieve results without taking as much risk, without spending as much money as you do in other forms of espionage. Therefore, this is very different from that point of view from other forms of espionage.

(b) Information warfare is very well known concept and need hardly be dwelt upon.

(c) Insider threat of course is the most difficult and most tricky aspect in cyber warfare and cyber security. Insiders have knowledge about your vulnerabilities and your configurations and it is easier for them to launch and to hide behind some anonymous sources.

(d) Hacking attracts press attention activities such as defacing websites etc. Most often they are more of a nuisance value than of any strategic military value, unless some people are careless enough to put sensitive information on their sites. But otherwise, the hacking of websites etc is not considered as major threat of cyber warfare. In fact, the people who want to resort to Cyber Warfare rarely want to be seen or heard.

(e) Then there are the **Hacktivists** who have some political or social objective or some religious objectives based on which, they do hack into sites and post say their messages. Of course, they also command more of a nuisance value with a difference that they are more organised. So sometimes their potential damage can be much more than the random freelancers.

(f) There is another breed that one should be very careful about. There are a few people whose **profession is writing 'virus software'**. This is a very standard threat that many of us face without knowing it.

(g) Criminal groups indulge in cyber crime and it is a source of huge economic losses to the industry. Every year billions dollars worth of losses are reported across the world because of criminal attacks in the Cyber Space.

Now coming back to views on cyber warfare, there are two views: James Lewis calls these Cyber Weapons as weapons of mass annoyance. During the Second World War and after that, a survey was conducted on the

effectiveness of strategic bombing on Germany. They felt that such an onslaught will be so disastrous that it would paralyse and cripple their entire military and economic machinery. But, interestingly, what they discovered was that the industrial production actually increased during the two years under the bombing. The reason was the resilience of the system and its ability to adapt. They found ways and means of averting and circumventing the problems created by the bombing. So, his argument is that even if the infrastructure is attacked in the warfare context, ways and means are found to avert and circumvent the problems and the attacks may not be as effective as people are making them out to be. In his view, “Information warfare and information security have become critical elements in successful military operations. But no nation has placed its military forces in a position where they are dependent on computer networks that are vulnerable to outside attack. This greatly limits the effectiveness of cyber weapons.” So according to this school of thought, they felt that Cyber attacks are not as much of a catastrophe as projected.

“Cyber attacks however do have a potential for imposing an economic cost far out of proportion to the price of launching the attack” as I was mentioning in the case of espionage. This brings in the other view viz., “The average annual cost from tornadoes, hurricanes and flood damage in the US is estimated to be 11 billion dollars. In contrast, the Love Bug Virus – one of the viruses which were used in attacking a lot of networks in the US and other countries as well, is estimated to have cost computer users around the world between 3 to 15 billion dollars – just one virus.” This is pure economic cost in terms of loss of time and information and all kind of outages that might have been created, and customer compensations companies might have had to make. So on this issue, there is total consensus among all the people, that as a tool of economic/ commercial warfare, it is a tremendous asset. Many experts believe that digital pearl harbours are unlikely because infrastructure systems have to be necessarily resilient. They deal with the failures on a routine basis and have mitigating strategies in place and are designed to be more flexible and more responsive. These are the issues which are generally applicable to the industrial society and may be to others to a different extent.

As internet and internet based economy or network based command and control systems and weapons control systems grow, the vulnerability to Cyber attacks increases. as long as Networked Systems exist, vulnerabilities will exist. In theory, every networked system is potentially vulnerable.

Let us see, what are the doctrines or views, expressed in different countries on cyber warfare. It is clarified here that the views brought out here are not necessarily their official line. In some Russian literature very strong views are expressed. “From a military point of view, the use of information warfare against Russia or its armed forces will categorically not be considered a non-military phase of a conflict whether there were casualties or not . . . Considering the possible catastrophic use of strategic information warfare means by an enemy, whether on economic or state command and control systems, or on the combat potential of the armed forces . . . Russia retains the right to use nuclear weapons first against the means and forces of information warfare, and then against the aggressor state itself”.

If you look at China, very interesting views are put forth. Cyber warfare is seen as a “transformation from the mechanised warfare of the industrial age, to a war of decisions and control, a war of knowledge and a war of intellect.”2 The Chinese concept of Cyber Warfare incorporates the unique Chinese views of warfare based around the peoples’ war concept. Much of their emphasis in their approach is on deception, knowledge style war and seeking asymmetrical advantage over an adversary. In my view they have a strategy and they are implementing it in right earnest. Continuing the views from China, Qiao Liang and Wang Xiangsui of PLA, in their book “Unrestricted Warfare”, claim that “warfare is no longer strictly a military operation and that the battlefield no longer has boundaries”. The authors also assert that “war has not disappeared, but its appearance has changed and its complexity has increased”. (Not an officially endorsed policy, but seems to have some degree of acceptance). A statement attributed to Chinese Major General Wang Pufeng in 1995 states, “In the near future, information warfare will control the form and future of war. We recognise this developmental trend of information warfare and see it as a driving force in the modernisation of China’s military and combat readiness. This trend will be highly critical to achieving victory in future wars.”

The USA is leading from the top because they are more often than not, the technology creators and the technology drivers. Their Joint Vision 2020 states that the continued development and proliferation of information technologies will substantially change the conduct of military operations. And that the changes will make information superiority a key enabler. Recently, they have also created 24th Air Force and US Cyber Commands. Apparently this is the first published establishment of Cyber warfare in the USA and it joins the historic domains of land, sea, air and space.

Supply Chain Control is another very important aspect. When we buy systems, sub-systems, components etc for use in our critical infrastructure that have cyber electronics component, they could sell these with vulnerabilities built into them, without your knowledge of course. And they can exploit them when they need to. The British donation of Enigma cipher machines to other nations after World War II was reportedly with the intent to gather information these nations were passing through. According to some reports, system controller devices brought from black market in the Soviet Gas Network is another case. Apparently during cold war, the Russian company wanted to get the American sub systems, but being a communist country, they were banned for export. They therefore, purchased sub systems and components from the black market which were reportedly incorporated with certain vulnerabilities in them by the supplier, designed to malfunction when required which would lead to pipeline explosions. This is a point that has been made public after the Freedom of Information Act was passed. We do not know whether they were actually operated during Cold War to create any destruction but certainly there existed the potential.

No discussion on Cyber Warfare will be complete unless one mentions about the recent events in Estonia and Georgia. The unprecedented electronic attacks on Estonia in May of 2007 clearly bring out the dangers. When Estonian authorities began removing a bronze statue depicting a World War II-era Soviet solider in Tallinn

(capital of Estonia), the internal protests were insignificant compared to the external response that far exceeded their wildest expectations. What followed was what some have described as the first war in cyber space, a month-long campaign that has forced Estonian authorities to defend their nation from a data-flood that they claim was initiated on orders from Russia. The Russian government denied any involvement to the attacks that came close to shutting down the country's critical digital infrastructure by clogging the websites of the President, the Prime Minister, Parliament and other government agencies, as well as staggering Estonia's biggest bank and the sites of several daily newspapers. Most of the attacks were of the DDoS type (Distributed Denial of Service) using a giant network of zombies machines or so-called botnets that included perhaps as many as one million computers. These botnets greatly amplify the impact of this type of assault. As a sign of their considerable resources, there is evidence that the attackers rented time on other botnets. According to sources, the 10 largest assaults blasted streams of 90 megabits of data per second at Estonia's networks, lasting up to 10 hours each. That is a data load equivalent to downloading the entire Windows XP operating system every six seconds for 10 hrs. The cyber attacks in the Baltic state of Estonia in early 2007 managed to disrupt that country's financial system for a few weeks; however, it did not destroy it.

International Laws on Cyber Conflict and Rules of Engagement. Mr Hollis, one of the experts in cyber warfare opines that under international law, a country that considers itself the victim of an act has a right to self defence with conventional military (not merely electronic) means. In other words, if you define a particular act in cyber space as cyber war, then you have the right to retaliate even if it means retaliation through conventional war. So, this is the reason why it is felt that there should be a much clearer and a definite set of international rules and conventions. In land, sea and air battles, international boundaries are easily defined. When somebody enters your territory with force, it is a very clear event and can be easily seen. It is not so in Cyber Warfare. In addition, the international community has defined things such as, when an adversary's use of force threatens a nation's territorial integrity and political independence etc. No such concept exists in Cyber War.

There is another view. I think this is a more liberal view. Cyber space relies heavily on other physical domains to operate, and International laws exist that govern the physical domains but when you are sending a malware to another country – via X country to Y country, you are violating the laws of that country as per the existing laws. But the question is how to operate the law in this case. It is not easy. The far reaching nature of cyber space generates jurisdictional challenges and as we have mentioned that it traverses through so many countries. Nobody can easily decide in Cyber Warfare whether it is a civilian violation or military violation.

Now coming to the Indian IT Scenario: There is huge amount of growth in State Wide Area Networks (SWAN's) – internet in other words. 25 mission mode projects are coming up in economic and industrial area. This is in addition to the private industry which is itself having huge operations, and setting up huge networks. If a large Indian IT industry is threatened, it is a national threat. Whether private or public, this entire network is critical from National Security point of view. Unfortunately, security is not high on our priorities in most cases.

In the Indian context, we also have near total reliance on external sources for hardware and software which includes operating systems, application software and most importantly all anti-virus, network protocols, computer and network hardware components et al.

Here again, there is a conflict of interest between economic growth and security and as always, economic growth takes precedence over security. Unfortunately, that's the reality.

Now I have come to the other aspect of cyber war, which not many people talk about. Hardware is as much susceptible to cyber warfare as software. Back-doors and malicious circuitry can be hidden inside counterfeit hardware and software - all the way down to 'Basic Input Output System' and instruction-sets inside of integrated circuit chips. It provides a covert attack vector and can be exploited.

The Israelis reportedly bombed a Syrian radar base in 2007. After this was done, there was a lot of debate amongst the professional bloggers and security experts about the incidence as reported in the Instiute of Electrical and Electronic Engineers (IEEE) spectrum. The Syrian radar could not detect the coming of Israeli aircraft. Bloggers have a view on this. What they say is that this Syrian radar has been fitted with a kill switch, a kind of vulnerability in the hardware and at the time of attack, this particular vulnerability was activated and the radar was rendered useless. They have speculated that the 'Commercial Off The Shelf' microprocessors in the Syrian Radar might have been purposely fabricated with a hidden "Backdoor" inside. By sending a pre-programmed code to those chips, an unknown antagonist had disrupted the chips' function and temporarily blocked the radar. There is of course no proof for this. Even the US is concerned about this because a lot of US manufacturing is outsourced to China and other countries. It has become a big issue now for the USA too.

As a result of all these hardware related concerns the US DOD have recently launched a programme called Trust in Integrated Circuits Program. This programme is meant for establishing very large sophisticated and trusted facilities to test critical electronic components for such hidden bugs. If the Americans are doing that and spending so much money, then it surely means something and we must take note of this too.

Of course, countries like us may not be able to spend that kind of money. We should use our ingenuity. We should use our own native talent and do our best to mitigate this problem and act together as a nation. Most essential for any form of resilience is a full understanding and control over the technologies and systems of the infrastructure, cyber security awareness and education. So, lots of effort must be put into analysing and understanding nuances in these areas. At least some of the components and sub-systems which we import must be thoroughly tested. We must ensure that all critical systems use components only from a selected parts list which has gone through this kind of analysis.

Sanitisation techniques and strong cryptography, good security enabled commercial information technology etc.

are very important. This is one simple way of ensuring security of critical information. It must be increased manifold. We simply do not have even a fraction of what we need in India. This must be tackled on a very large scale.

We may not become a super power in hardware, but at least we can take care of many things that are critical if we can get our act together and in time. Security Software engineering and software assurance is still not a very profitable profession in India. The latest IT act amendment addresses this issue. It calls for the establishment of separate nodal agency for critical information infrastructure protection. These things would hopefully alleviate some of the dangers that we face.

As regards, what the future portends? Tools and techniques of Cyber Warfare are presently accessible to non-state actors and other technologically less endowed entities – giving them certain advantage of asymmetry. There are no super powers in Cyber space currently. Anybody who has knowledge and techniques can be a super power as it stands today.

In future however, we can expect a concerted effort to lift this total paradigm to much higher levels of technology and sophistication in order to deny this advantage to the lower-technology level entities. This will happen through the use of new generation hardware and software. There will be a shift in the battle from something that is accessible to everybody to only a select few. This would also ensure continued and much stronger advantage in favour of the technologically advanced countries.

Future Cyber War Scenarios

Scenario 1: Sustained strategic low – intensity economic Cyber Warfare. You will not even know about this. A large numbers of companies are there which are not so well protected on the internet but they deal through internet. So technologically superior countries can clandestinely access and get their business secrets. If it is done strategically for a sustained period of time, most productive companies can go bust and that will be an economic calamity for the affected nation.

Scenario 2: Supply chain controlled disruption / destruction of vital assets in times of crisis - you remain blissfully ignorant and continue to work with otherwise sophisticated components and sub systems, but when the day comes, you may not have the necessary safeguards to protect against a directed attack that exploits the deliberately hidden vulnerabilities.

Scenario 3: Supply chain controlled disabling of C3I and other military systems

Scenario 4: Strategic espionage for economic, military and political objectives.

All this is going on simultaneously. You must have heard what China is doing and there is nothing to stop them unless we keep developing our prowess in Cyber Warfare together with other ingredients of Comprehensive National Power. Integration of communication technologies with the internet would further increase the challenges dramatically.

Thank you.

---

* Text of the talk delivered at USI on 21 October 2009. Dr VK Singh was in the Chair.

Shri KVSS Prasad Rao is the Chairman, National Technical Research Organistaion (NTRO) and Ex Officio Secretary to the Government of India. He is also an honorary Scientific Consultant in the office of the Principal scientific Adviser to the Government of India.

Journal of the United Service Institution of India, Vol. CXXXIX, No. 578, October-December 2009.