Cyber Warfare & National Security Strategy*

Shri PV Kumar**

Introduction

Lieutenant General PK Singh, Director USI, distinguished members of the USI, members of the academia, diplomatic and press corps, ladies and gentlemen; I consider myself privileged to be here amongst you to deliver the Eleventh Major General Samir Sinha Memorial Lecture on the subject of 'Cyber Warfare and National Security Strategy'. I am thankful to USI for giving me the opportunity to speak on an issue of such contemporary relevance and importance. As Chairman NTRO, I feel a particular sense of criticality and urgency towards the issue. The topic is so vast and complex that an address of this nature may not be able to do full justice to it.

I would like to emphasise that what I say today are my personal views which do not necessarily represent the views and official position of the Government of India. While addressing today's gathering of soldiers and strategists, I will try and focus on those aspects of Cyber Warfare and National Security Strategy which would interest you. First and foremost, one is convinced that Cyber Space has blurred all conceptual and physical boundaries as we understand them in the field of warfare till now. I will briefly touch upon the evolution of society and warfare.

Human society has in the last 500 years witnessed by and large three phases of socio-technical revolution covering the periods of the 1st and 2nd Industrial Revolutions and finally the current Information and Communication Technology (ICT) Revolution. Social structures, governance and warfare have also undergone evolution in sync with these phases of our society. It may not be incorrect to say that nothing like ICT has ever been witnessed by human society – in terms of technology itself, its impact on all aspects of our lives and the pace of change that it has precipitated.

At the core of the ICT Revolution is the ever crucial, abstract, intangible commodity – information; whether it is data, intelligence, knowledge or wisdom. Information is a virtual commodity, having some rather unique attributes. It can be shared without its value being reduced. It can be stolen and is not measurable. The same information can exist in more than one place at the same time. It is non linear in its impact; small quantities can have large effects.

Impact of Information and Communication Technology

In today's world ICT is omnipresent and it pervades every aspect of our lives. State-of-the-art technology, ever-improving performance and tumbling costs have resulted in widespread proliferation of ICT. The ICT revolution has changed the world to a border-less entity compelling the creation of a new world order. The Internet as a network of networks has reshaped large parts of the world as a borderless world of convergence between communication and computers resulting in an unprecedented integration of peoples, structures and processes.

ICT has enabled the efficient collection and use of information. Various elements like processing machines, storage devices and communication networks etc form its core components. The large presence of ICT in public infrastructure, both critical and non-critical, has emerged both as a benefit and a threat. The technology trajectory has resulted in an ever increasing social dependence on ICT structures and mechanisms as never before. Today technology has brought ICT within the reach of the un-initiated which has resulted in its wide social impact. The Social Networking and Mass Communication systems have networked societies and individuals as never before. On the business side, ICT is today the lead money spinning industry. With these attributes, ICT and its related infrastructure have now become critical assets. And like any other national asset, ICT has become an important target for adversaries as well.

As warfare experts would like to say, ICT now forms the 5th or 6th most critical dimension of modern warfare, depending on how one differentiates between electronics and Cyber Space technologies.

Cyber Space and Cyber Warfare

That brings us to Cyber Space, which though an offshoot of ICT, has now assumed an identity of its own. Like ICT, Cyber Space too has assumed huge proportions. ICT and Cyber Space have offered new frameworks for functional interoperability between all forms of human and Electromagnetic interactions. It is no longer a high tech venture which used to be the exclusive preserve of scientists and technologists. An important evolutionary aspect of Cyber Space is that it has emerged as a largely de-regulated medium. This has presented a new challenge to certain societal aspects which includes governance, the threat landscape and security.

Though nation states do often attempt to create regulatory structures, the Internet seems to have defeated most such endeavours, atleast till now. Like ICT, Cyber Space has become an important national asset spanning across all sectors, including governance and security. New capabilities have enabled new threat vectors for Cyber enabled warfare and Cyber Warfare itself. It has made the commission of crime easier and crime detection even more complex. While it is not my intention to over state its importance, Cyber Warfare is likely to decisively influence the pre-conflict stages and eventually the outcome of conflict itself. We need to appreciate that due to the omnipresent nature of ICT and Cyber Space, it is possible that this may lead to a new form of National and Total War.

Some distinctive features of Cyber Warfare are :-

(a) Cyber Warfare can enable actors to achieve their political and strategic goals without the need for armed conflict.

(b) Cyber Space gives disproportionate power to small and otherwise relatively insignificant actors.

(c) Operating behind false Internet Protocol addresses (IPs), foreign servers and aliases, attackers can act with almost complete anonymity and relative impunity, at least in the short term.

(d) In Cyber Space the boundaries are blurred between the military and the civilian, and between the physical and the virtual; power can be exerted by states or non-state actors, or by proxy.

Cyber Space can be viewed as the 'fifth battle space', alongside the more traditional arenas of land, air, sea and space. Cyber Warfare is best understood as a new but not entirely separate component of this multifaceted conflict environment. Warlike actions in Cyber Space are more likely to occur in conjunction with other forms of coercion and confrontation. However, the ways and means of Cyber Warfare remain undeniably distinct from these other modes of conflict.

It is said that 'war' and 'warfare' have an 'unchanging nature', yet they have a 'highly variable character': 'We know with a sad certainty that war has a healthy future. What we do not know with confidence are the forms that warfare would take. Although the concept of revolution in military affairs (RMA) is typically associated with technological advancements, it also involves changes in strategy, operations and tactics. With the dominance of information in all spheres, new strategies would keep evolving in both defence and offence.

The growing relevance of Cyber Warfare in RMA is on expected lines. At the turn of the century, the Pentagon adopted the doctrine of Network-Centric Warfare (NCW) and set out its vision of autonomous 'swarming' and 'self-synchronised' war fighting units connected to one another by high-speed data links and superior battlefield awareness. This brings us to the 'chaoplexic' form of warfare fought by decentralised networks.

Military theorists allude to the 'swarm', the networks of distributed intelligence that enable bees, ants and termites to evolve complex forms of collective behaviour on the basis of the simple rules of interaction of their individual members. Of particular interest are the resilience and flexibility of these swarms as amorphous ensembles whose continued existence and successful operation is not critically dependent on any single individual. Military swarms promise not only more adaptable and survivable forces but also new offensive and defensive tactics better suited to the contemporary battle space. Beyond the flexibility and evolutionary capability, it is also claimed that military swarms can converge on their target from all directions in offensive bursts, thereby maximising the shock effect.

Hostile actors in Cyber Space can make use of a wide range of techniques. Malicious software (malware), networks of 'botnets' and logic bombs can all be employed to navigate target systems, retrieve sensitive data or overrule command and- control systems. Although the technology and skills involved in designing, building, testing and storing these weapons may be complex and advanced, the means by which the weapon is delivered and by which the desired damaging effect is caused may be astonishingly simple. One well-known example occurred in 2008 when highly classified US Department of Defence (DoD) networks were reportedly infected by an unknown adversary that 'placed malicious code on USB thumb drives and then dispersed them (in parking lots) near sensitive national security facilities. After a curious finder inserted the drives into computers, the code spread across their networks.

Let us examine the direct military threats emanating from Cyber Space. Cyber technology has clear military applications which can be exploited in conflict situations. Whether through military equipment and weapons systems, satellite and communications networks or intelligence data, the armed forces are highly dependent on information and communications technology. While it provides immense advantages it also throws up major challenges in terms of information overload making assessments difficult. Bombs are guided by GPS satellites; drones are piloted remotely from across the world; fighter planes and warships are now huge data processing centres; even the ordinary foot-soldier is being wired up. In a digital, knowledge-based society this is to be expected. But while technology brings opportunities it can also create vulnerabilities. The major powers have long recognised the strategic and tactical value of Cyber Space. Similarly, weaker states are now seeking to partially offset this asymmetry by developing their cyber capabilities. Military strategists have come to view information dominance as the precursor for overall success in a conflict.

Impact on National Security and Warfare

The nature of Post-Modern Conflict has undergone a huge change, especially since the Gulf Wars and 9/11. Both state and non-state actors have achieved threat parity and terrorism is likely to dominate the conflict scenario. Cyber Warfare has emerged as an important new element of warfare. Cyber Warfare is arguably at the most serious end of the spectrum of security challenges posed by – and within – Cyber Space. Just like the tools of conventional warfare, cyber weapons can be used to attack the machinery of a state, financial institutions, national energy, transport infrastructure and even public morale. ICT and Cyber Space have had a profound effect on the affairs of the state. Free flow of information across TV screens, e-mails, cyber chat rooms etc contribute to wider event awareness, debate and transparency. Who could have imagined the Arab Spring and Shahbagh movements 20 years ago. But the Information revolution generates its own contradictions. It strengthens forces of both anarchy and control.

From what we see today as part of youth movements powered by Social Media, the individual has become more empowered as compared to social and government structures. Many hierarchies lie destroyed and are being replaced by new and more broad based power structures. The ICT revolution also offers too many choices, greater insight and has the potential to increase the fog – both in peace and wartime. As was brought out earlier, ICT or Cyber Space structures have become vital national assets.

The National Information Infrastructure, including computers, networks, storage devices, communication systems, cyber enabled and cyber controlled systems etc, has assumed an importance unheard of before. As has been shown in many Hollywood movies, cyber linked physical infrastructure is now a genuine target of physical destruction or disablement through cyber means. Hardware is just as susceptible as software. Backdoors and malicious code or circuitry hidden inside counterfeit hardware and software, all the way down to the basic input-output system (BIOS) and instructions set inside the integrated circuit chips is a case in point. Any vulnerability in the BIOS of microprocessors can be exploited to gain control over the computer. The design, manufacturing and testing stages of IC production are done in a diverse set of countries. This makes quality control a difficult proposition. With commercial off-

the-shelf (COTS) procurement and global production, there is an increasing risk of covert hardware/firmware based cyber attacks. Most of us know what a digital worm or a virus like Stuxnet can do to the physical world of Supervisory Control and Data Acquisition (SCADA) controlled systems. Aviation, railways, power systems, food supply chains, R&D facilities, e-governance structures are today vulnerable in a threat mosaic never encountered earlier.

ICT's impact on financial systems including banks, stock-exchanges, electronic fund transfer mechanisms, e-commerce architectures etc has resulted in new threat and security frameworks. Defence assets, structures and related vulnerable areas and vulnerable points are under severe threat today, both during peace and wartime.

Let us now look at what is under threat in the world of ICT itself. The Internet population has jumped from 1.15 billion users in 2007 to 2.27 billion in 2012; i.e. it has almost doubled in five years. The largest and fastest rising numbers are in Asia with India and China at the top is no surprise. In an Internet minute, nearly 1 terrabyte of data is shipped, 1300 new mobile users added, 204 million e-mails sent, more than 6 million Facebook views generated, more than 2 million search queries on Google, 62000 hours of music transacted, 30 hours of video uploaded and 1.3 million video views generated on Youtube.

For people of my generation this sounds mind-boggling. But let us get shocked further. Today the total number of networked ICT devices equals the world population. By 2015 these will be twice the world population at that time. Today Global IT revenues have exponentially jumped from USD 350 million in 1997 to around 120 billion in 2012. In all, including services, telecom etc, ICT can be valued at around 6.8 trillion dollars.

Issues

The Internet technologies, which employ open standards for exchange of information and have made this mind boggling scale of things possible, are not fundamentally secure. This fact, as a result of which systems remain ab-initio vulnerable, needs to be appreciated when studying the security aspects. The systems were made even more vulnerable due to compromises affected for commercial convenience and making them user friendly.

The threat to information infrastructure today spans processing elements, storage systems, transmission networks etc. On the other hand, easy availability of information to the adversary poses a challenge which has to be dealt with without affecting own systems. Today cyber enabled Information Warfare has further enhanced the threat to the decision making process through more efficient information disruption and misinformation mechanisms.

Social Media

The grievances in the Gaza War may be ancient, but some of the weapons reportedly being used are spanking new; reflecting the changed nature of war in this cyber era. One reads for example about a part of the war being tipped in a side's favour based on the number of Twitter posts far outnumbering those of the other side. Recently in Egypt and Libya, massive riots were led by extremists who were apparently united and who stormed embassies. Riots and demonstrations followed all over the world. It has been reported that the attacks on the embassies were executed in a coordinated manner on multiple embassies at the same time. The attacks were reportedly incited, spread and well coordinated through social media like YouTube, Facebook and Twitter.

Social media seemed to have been employed to stoke an insurgency. It illustrates how, often something innocuous can be get blown out of proportion by certain powers with an agenda using this new weapon in their arsenal. This level of social manipulation can be readily adopted by foreign powers to foment trouble well outside their own national borders. The magnitude, scale, apparent-spontaneity, decentralised nature yet well networked and coordinated nature of this attack - seem to fit well with the theories of 'Chaoplexic Warfare' mentioned earlier.

This may be the right moment to take a peep at the exotic world of Cyber threats and terms like hacking, phishing, Denial of Service Attacks, Botnets etc. Without going into jargon, these are various forms of threats and delivery systems. For example, as is apparent from the term, Denial of Service (DoS), is actually denying users a service mostly through inundating the Service Provider.

Botnets are groups of zombie computers under the control of a remote and invisible hacker forced to function in a manner not desired of them. Today hackers can control an army of bots all over the world which can be used to attack a system, a network or networks, a service or a nation. Can these zombie army of bots, involving your and my computers, be used to attack a nation. Yes, it is possible. Remember Estonia, where an entire nation was paralysed by a cyber attack. Estonia happened to be one of the most wired countries at that time.

When these bots are used to fire large cyber traffic to inundate an entire target infrastructure the DoS becomes Distributed DoS. This seems to have happened to the US banks recently. You may recollect what happened last month to the Spamhauss organisation which deals with anti-Spam operations. It was probably the largest cyber attack which has come to notice with thousands of Bots initiating millions of transactions on Spamhaus servers, effectively shutting them down and even slowing down the Internet. We all know how Stuxnet was used to disable the Iranian nuclear programme attacking the Siemens control systems deployed for operating centrifuges. Or for that matter the subsequent Flame virus which was focused on Middle East for information collection. Around 30000 bots were used to target Aramco of Saudi Arabia which is one of the largest oil producers. The production there was disrupted for many days.

Attribution and the China Bogey

The People's Republic of China (PRC), in particular, has long recognised the strategic and tactical value of Cyber Space. The PRC is believed to be focusing inter-alia on its cyber capabilities to counter the current military asymmetry with the USA in terms of military and technical hardware. Chinese military strategists have come to view information dominance as the precursor for overall success in a conflict.

A lot is written about China's prowess in the field – this is a possibility that cannot be denied given the fact that China has emerged as a formidable force in the world of technology. The Titan Rain attacks in 2007 – one of the most large-scale infiltration of the US and UK government departments, including the US DoD and the UK Foreign and Commonwealth Office – were attributed to China, and had allegedly been under way since 2002. Furthermore, in Mar 2009 China was linked to 'GhostNet' when it was revealed that a large-scale spying network had attacked a significant number of government departments and strategic targets, including the Tibetan community.

On 19 Feb this year, a report by the US-based Cyber Security firm Mandiant accused the Chinese military of being behind a series of cyber attacks against businesses, institutions and infrastructure in the US. That was not the first time that China received accusations of this type, although the novelty was that the report localised in detail the origins of the attacks. According to Mandiant, a Chinese army building in a suburb of Shanghai was responsible for most, if not all of the attacks.

Beijing categorically denied the charge adding that it is also the victim of numerous attacks, which have increased over the years and most of them are from the North American country. A computer security official said China had become the world's biggest victim of cyber attacks, with a report from a national computer monitoring centre revealing that many domestic computers were controlled via overseas-based IPs last year. A total of 47,000 overseas IPs were involved in attacks against 8.9 million Chinese computers last year, compared to nearly 5 million affected computers in 2010, according to a report issued by the National Computer Network Emergency Response Coordination Centre of China (CNCERT/CC), China's primary computer security monitoring network. Most of the IPs originated in Japan, the US and the Republic of Korea (ROK), according to the agency. Since attribution is very difficult in the cyber domain, it is difficult to conclusively support the argument that China is actually behind much of what is being witnessed.

Indian Cyber Scenario

In India, as we are all aware, there is a near total reliance on external sources for hardware and software (operating systems, application software, antivirus, network protocols et al). In view of this, it is virtually impossible to have complete information on hidden vulnerabilities such as the presence of trap doors and malware.

Some mitigation strategies could include those most essential for resilience, namely a full understanding and control over the technologies and systems of the critical infrastructure, cyber security awareness and education, sanitisation techniques and strong cryptography, good security-enabled commercial information technology, an enabling global security management infrastructure and a strategic push to investment in indigenous development/production of hardware and software. This needs a focus on Research and Development particularly in areas of : authentication technologies; secure fundamental protocols; secure software engineering and software assurance; holistic system security; monitoring and detection; mitigation and recovery methodologies; cyber forensics: catching criminals and deterring criminal activities; modeling and testbeds for new technologies; metrics, benchmarks and best practices.

Technology and R&D

Cyber technologies are a very new field as compared to other established technology areas. These technologies have matured over the last two decades or so. Hence there is a large need to develop not only secure cyber frameworks but also put in place defensive cyber technologies to guard against various threats which were mentioned earlier. It is an understatement to say that a fast moving R&D framework is the bed rock of any cyber security endeavour. As has been enumerated in some of the international cyber security documents, we require to develop R&D strategies to enhance the security, reliability, resilience, and trustworthiness of digital infrastructure. The R&D effort also needs to be coupled with technology forecasts to cater for immediate and long lead items.

There is a pressing need for developing technologies for various segments which include secure data communication technology, encryption frameworks, resilient and sustainable digital infrastructure, large scale realtime data processing systems, threat identification and intrusion detection systems etc. While the technologies, I just mentioned, have more to do with enabling mechanisms, the cyber defence and mitigation strategies require a parallel development effort to cater for containing the fallout of major cyber attacks. In addition, this also needs constant evolution to keep pace with the new types of cyber threats which are encountered on nearly hourly basis.

While development of technology has a dynamics of its own, a realistic appraisal of the available technologies and their likely trajectory, needs to be undertaken in a comprehensive manner. Such forecasting is required both for the enabling systems and from the cyber warfare point of view. This also includes constant and independent analysis and assessment of vulnerabilities in the existing systems, hardware, networks, processing elements etc. This is a very challenging task in its own right. A word about who needs to do all this.

Based on what we understand of the all pervasive nature of cyber space and its effect on all aspects and dimension of our societies, it is not possible for any agency, sector or government to go it alone. It is inescapable that various arms of government, academia and industry collaborate and coordinate efforts to cater for the demands of such a fast changing field. It can be appreciated that entities both within the government and outside have strengths of their own which are best suited to take on the respective areas of responsibilities.

Cyber Security Manpower

I would also like to emphasise on a very important related aspect. While we have talked so much about cyber technologies, its potential and dangers, it needs to be appreciated that it is finally the man behind the machine which is the most important factor for any success, especially in the cyber world.

The developments during the last one to two decades indicate that while sufficient expertise is available in

the field of exploiting cyber technologies, it is the cyber security expertise which is not available in the required numbers as yet. In addition, such expertise is also not available with the required capability levels. We need a constant supply of capable man power from academic institutions and industry to pitch in for defending Cyber Space. It is a long haul but an institutionalised start needs to be made; otherwise while developers would have created systems with enormous capabilities, defending such systems will lag behind which could result in a potentially disastrous situation.

Secure Technology Framework

The panacea for such a state is indigenisation and this is being aggressively pursued. We need to be able to develop world class products (operating systems, application software, hardware such as network components, even chips being used etc) that we can use with the kind of faith that comes from knowing everything about it. Greater awareness of Cyber Security aspects through training, information dissemination, adoption of best practices, regular cyber audits by experts etc would also contribute significantly. This aspect is of great strategic importance and needs active involvement of academic institutions, industry, think tanks and government institutions.

Cyber Space is also a global medium and we need to partner with our friends across the world. While some measures have already been initiated, India needs to actively participate in the international Cyber Security dialogue to safeguard our interests.

The Challenge

The scale of ICT applications and their openness which is conducive to growth, throw a sort of ‘grand challenge problem’ in protecting cyber assets from penetration and attacks. Cyber-attacks are now becoming the stuff that we read of at breakfast in our morning newspapers. In this regard I have already given examples of incidents reported in the recent past. A significant area of concern is cyber espionage which is the most prevalent of the cyber activities. Whether used to uncover sensitive government information, steal trade secrets or commercial data or as part of intelligence or reconnaissance work, it fits into the doctrine of using ‘information superiority to achieve greater victories at a smaller cost’.

Many nations are pursuing offensive cyber capabilities, but not much is revealed about this in the public domain. However, in a recent departure from this norm, Chief of the US National Security Agency recently disclosed that the US DoD is establishing a series of cyber teams to combat the threat of a digital assault that could cause major damage and disruption to the country’s vital infrastructure. He mentioned that 40 teams should be ready by 2015 and that 13 of the teams will be offensive fighters specifically designed to attack other countries while the other 27 cyber teams were being established to support the military’s warfighting commands. Some others will protect the Defence Department’s computer systems and data.

There can be a psychological dimension to cyber-attacks. The infiltration, of what are assumed to be secure systems and critical infrastructure, highlights national vulnerabilities and weaknesses. This can provoke feelings of insecurity which could indeed be the attacker’s goal; in the same way that the fear of terrorism and its potential harm can have a detrimental and disabling effect almost as great as the terrorist act itself.

Developed countries frequently complain about large scale espionage and surveillance operations by cyber attackers, with their defence and hi-tech industry as one of the prime targets. In the case of suspected state-sponsored actions it is difficult to establish beyond any doubt that the order to attack originated in the executive or presidential office, let alone a capital city. Furthermore, the difficulties of attribution allow a degree of plausible deniability. Perpetrators can cover their own tracks and implicate others, particularly when third-party servers and botnets in unrelated countries can be used to originate attacks and provide cover for the actual attacker. The increasing integration of National Information Infrastructure with military information infrastructure has diffused the boundaries between civil and military information networks.

Can we imagine what will happen to us in a situation like Estonia, the US or Saudi Arabia? Do we fully understand the threat? Do we have a measure of it, and are we prepared for it? Are we still working with archaic civil-military frameworks? Is there a difference between peace and wartime? Are we matching up with the faster information proliferation and propagation mechanisms leading to information flow management problems? Are our business models geared for the threat? Does the industry and the government’s L-1 system of procurement provide for the commercial vs security compromise? Do security overheads not often tempt us to opt for relatively unsecured but operationally capable systems for ease of operation and management? All I can say is that policy frameworks are in the process of being put in place to address such issues.

Policy Options

Never in the history of national security management have such high demands been placed on information collection mechanisms which need to process such large amounts of data and at such high speeds. A 24x7 situational awareness and matching fast paced mitigation mechanism can not be delayed any longer. However, this may agitate some privacy advocates who may be justified in treating national security threats and privacy at par. I would like to bring out that there are enough comprehensive frameworks available in Indian laws and the IT Act to arrest such negatives. Similar examples are available across the world like the legal formulations in the US and the UK. The European Union is also evolving its own version for a multilateral and multi-nation framework. It may require a full discussion to dwell upon the various dimensions of the legalities in ICT.

Recently, the US had initiated a series of policy measures with their President pushing it past the Congress. There could be lessons for us also. The policy framework needs to address the immediate and futuristic requirements; as the threat is here and now our adversaries, whether state or non-state actors, are already on the job. A national level coordination effort at policy and operational levels is the foundation layer for any cyber security endeavour. India needs a national cyber coordination mechanism for threat assessment. This should have multi-agency participation. Some

efforts in this direction have already been initiated. This endeavour will result in a credible Information scanning framework in coordination with the service providers and industry.

In order to make sense of it all, a comprehensive data analytics capability with mining and fusion mechanisms needs to be put in place for predictive trend analysis. Such skill sets need to be honed with advanced simulation and modelling techniques. A large body of research work already exists in this area which is waiting to be absorbed. While information collection and predictive efforts fall in the pre-event category, measures will require to be put in place for the post-event phase also.

Its time we touch upon the mitigation strategies also. This will involve counter measures and realtime forensics. The mitigation and counter measure aspects need to be handled in a coordinated manner at the national level. We need to prepare a Cyber Security Incident Response Plan and enhance public-private partnerships. While so much needs to be done at the operational level, there exists a very large need for cyber threat awareness, both within and outside the government. There is a need to initiate a national awareness and education campaign to promote Cyber Security. This basic measure needs to be undertaken at multiple levels of society and governance.

National Centre for Critical Information Infrastructure (NCIIPC)

Now I will briefly mention about the NCIIPC. The amendments made to the Information Technology Act in 2008 reflected the nation's recognition of the need to adopt an institutional approach to enhancing our cyber security profile as also to take steady but sure steps towards protection of its critical information infrastructure. The IT Act envisaged the creation of a specialised body to synergise our collective efforts and capabilities to protect the Nation's critical information infrastructure.

Critical sectors as you are all aware, are those sectors whose incapacitation or destruction would have a debilitating impact on national security, economy, public health or safety. Several initiatives have been launched in recent times to enhance our cyber security profile. The creation and activation of the NCIIPC for protection of our critical information infrastructure is one of the important components of this construct.

Conclusion

In conclusion, I may say that Cyber Space offers mind boggling opportunities for improving the quality of life and work but it also provides a threatening landscape for destroying it. There is no escape from Cyber Space or its threats. Society, visionaries, technologists and the Cyber Space 'Subscribee' citizen need to pitch in. Many old paradigms are no longer relevant. New frameworks need to be put in place with no loss of time. The Cyber world is all about speed. We can't afford to be left behind.

* Text of the talk delivered at USI on 10 Apr 2013 with Lieutenant General Prakash Menon, PVSM, AVSM, VSM (Retd), former Commandant National Defence College, New Delhi and presently, Adviser National Security Council Secretariat (NSCS), in the Chair.

****Shri PV Kumar** is a career intelligence officer. He joined the Research and Analysis Wing (R&AW) in 1971 and held important appointments in that organisation, both within India and abroad. He joined the National Technical Research Organisation (NTRO) in Oct 2009 as Senior Adviser and Deputy Chief of the Organisation. He took over as Chairman, NTRO on 31 Mar 2011.

Journal of the United Service Institution of India, Vol. CXLIII, No. 592, April-June 2013.