INDIA'S CYBER WARFARE STRATEGY IN NEXT DECADE

M.K. SHARMA

Attack is the secret of defense; defense is the planning of an attack.
— Sun Tzu, *The Art of War*

INTRODUCTION

The world is witnessing a remarkable shift in the locus of global power with the relative decline of the United States of America and the dramatic rise of China. It is estimated that the rise of India and China will alter the nature of the global system and the global landscape in the coming two decades. During this great geo-political transition period, there is an urgent need to revaluate our theories, paradigms, assumptions and strategies in the light of technological, economic, political and military developments in the region. The heavy dependence of government organisations, business, economic activities and military affairs on Information and Communication Technology (ICT) necessitates incorporation of cyber technology into our strategic calculations. Cyber power is exerting itself as a key lever in the development and execution of national policy, including counter-terrorism, economic growth, and diplomatic affairs. The US–China power competition in the region places extraordinary demands on India to enhance its power and influence primarily for the defence of its own sovereignty, territorial integrity and promotion of the global good while it builds up its economy

Wing Commander **M.K. Sharma** is a Research Fellow at the Centre for Air Power Studies, New Delhi.

Cyber power is exerting itself as a key lever in the development and execution of national policy, including counter-terrorism, economic growth, and diplomatic affairs.

and long-term prosperity, ironing out domestic inequities. Towards this, cyber power has the ability to create synergy with other elements and instruments of power and integrate them in a way that improves them all. For the next decade or so, cyber power can also be leveraged as an instrument of foreign policy to offset India's inadequate hard power, taking advantage of the expertise and human resource in the domain of ICT. Therefore, it is imperative to craft a cyber strategy that enables the exploitation of the capabilities that cyber space offers, while simultaneously protecting and defending against the vulnerabilities it presents.

This paper seeks answers to why the cyber weapon cannot be deployed and used like another kinetic weapon without the support of an apt strategy. And why (or why not) India should pursue cyber warfare more aggressively and, consequently, the paper explores how cyber offence, defence and deterrence options relate to form the national cyber warfare strategy.

UNDERSTANDING THE NEED

Strategy is defined as "the art and science of developing and employing instruments of national power in a synchronised and integrated fashion to achieve theatre, national and/or multinational objectives"[1]. However, when we approach a particular operational domain, the strategy is to be grounded in that realm; accordingly, cyber strategy means development and employment of strategic capability to operate in cyber space, integrated and coordinated with the other operational domains (land, sea, air and outer space), to achieve or support the achievement of objectives across the elements of national power, in support of the national security strategy.[2] Therefore, the key challenge to a national

1. Joint Publication (JP) 1–02, *DOD Dictionary of Military and Associated Terms* (Washington, DC: The Joint Staff, August 31, 2005).
2. Daniel T. Kuehl, *Cyber Power And National Security* (New Delhi: Vij Books, 2009), ch. 2, p 40.

cyber strategy would be to clearly demonstrate how it will integrate with, and support, other domain specific strategies and, consequently, the national security strategy to achieve their critical and interrelated objectives.

Cyber strategy means development and employment of strategic capability to operate in cyber space, integrated and coordinated with the other operational domains (land, sea, air and outer space).

Let us ask ourselves some basic questions as a starting point to arrive at a cyber strategy: is the advent of cyber warfare a good thing, or does it place India at a disadvantage? Do we envision the use of cyber war weapons only in response to the use of such weapons against us or are cyber war weapons something that we will employ routinely in both large and small conflicts? Do we see cyber space like other domains (like sea, air space or outer space) in which we must be militarily dominant and in which we will engage an opponent while simultaneously conducting operations in other domains? Should we be hacking into other nations' networks in peace-time? If so, should there be any constraints on what we would do in peace-time? What do we do if we find that another nation has hacked into our networks in peace-time? What if it left behind logic bombs in our infrastructure networks? Do we intend to use cyber weapons primarily or initially against military targets only, and if so, how do we define military targets?[3]

Further, some more important questions that the cyber warfare strategy should enquire into are: what is the importance of avoiding collateral damage with our cyber weapons? How might avoiding it limit our use of the weapons? What level of command authority should authorise the use of cyber weapons, select the weapons and approve the targets? Also, how do we signal our intentions with regard to cyber weapons in peace-time and in crises? Are there ways that we can use our possession of cyber weapons to deter an opponent? And, finally, if an opponent is successful in launching a widespread, disabling attack on our military or on our

3. Richard A. Clark and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About it* (Echo, April 2010), ch. 5. pp. 152-154.

economic infrastructure, how does that affect our military and political strategies?

In order to arrive at any useful cyber strategy based on the principles of war, it would be prudent to note that we are analysing a 'virtual world' with all its unique characteristics.

LOOKING THROUGH THE PRISM OF 'PRINCIPLES OF WAR'

Historically, military intellectuals have developed a set of principles of war to support the planning and execution of operations. These principles have evolved over hundreds of years through the writings of key military analysts.[4] India's principles of war are Selection and Maintenance of the Aim, Offensive Action, Maintenance of Morale, Security, Surprise, Concentration of Force, Economy of Effort, Flexibility, Cooperation, and Sustainability, as inherited from the UK.[5] These principles are based on the work of Maj Gen J.F.C. Fuller. Although there are country specific variations in the elements of these principles, the list revolves around unity of command, objective, offensive, mass, manoeuvre, economy of force, security, surprise and simplicity. In order to arrive at any useful cyber strategy based on the principles of war, it would be prudent to note that we are analysing a 'virtual world' with all its unique characteristics. Further, to evaluate the effectiveness of that strategy, we need to evaluate the ways and means available to the nation-state. Therefore, how this process can be applied to cyber warfare needs further illustration.

When we consider cyber warfare, do we see it happening only in the virtual battlefield or as being enmeshed into the physical battlefield too? While some of the principles of war don't easily transfer into the virtual battlefield, they can be force multipliers in the physical battlefield.[6] When

4. Carl Von Clausewitz, *On War*, ed. and trans, Michael Howard and Peter Paret (Princton University Press, 1975).
5. Air Vice Mshl Arjun Subramaniam AVSM, *Basic Doctrine of the Indian Air Force 2012*, ch. 3 pp. 13-16. http://merln.ndu.edu/whitepapers/India_Doctrine_Air-Force_ENG_2012.pdf
6. Janson Andress and Steve Winterfeld, "Cyber Warfare: Techniques, Tactics and Tools for Security Practitioner" in *What is Cyber Warfare* (Syngress,2011), ch. 1, p. 6.

deciding on a cyber warfare strategy, it would not be prudent to throw away our time-tested doctrines and tactics—rather, we should be able to modify them, based on the new realities brought in by the ICT. While keeping selection and maintenance of aim paramount with a plan that produces surprise is still the key to success, we need to ponder on whether offensive action is still the best way to achieve victory in the realm of cyber warfare or is there a requirement of reassessment of the appropriate principles of contemporary warfare?

In fact, there is already a debate on about having a revised set of modernised principles of warfare as appropriate for 21st century operations. Charles Dunlap has updated the list to include Perceived Worthiness, Informed Insight, Strategic Anchoring, Durability, Engagement Dominance, Unity of Effort, Adaptability and Culminating Power.[7] Table 1 shows the interrelation and linkage of the modernised principles to the classical principles of war.

Table 1

Modernised Principles	**Relationship to Traditional Principles**
Perceived worthiness	Moral: what makes it worthwhile to risk one's life in combat?
Informed insight	Sense making, cognition, surprise.
Strategic anchoring	Concentration on, and prominence of, offensive.
Durability	Incorporates security into plan; depend on logistics.
Engagement dominance	Incorporates and simplifies manoeuvre; imposes/ opposes surprise.
Unity of effort	Draws on unity of command; reinterprets economy of force, mass, manoeuvre.
Adaptability	Presupposes flexibility but does not mandate simplicity.
Culminating power	Power needed to attain satisfactory closure at a given level of conflict.

Source: Charles J. Dunlop, "Neo-Strategicon: Modernized Principles of War for the 21st Century", *Military Review,* March – April 2006.

7. Charles J. Dunlap, " Neo-Strategicon: Modernized Principles of War for the 21st Century," ***Military Review,*** March-April 2006.

It may be difficult for the leadership of one cyber power to determine when, in the mind of its enemy, it has crossed the line between cyber operations that are "acceptable" and those that will trigger a major escalation in the intensity of cyber activity.

NEW REALITIES AND ROLE TRANSFORMATION OF MILITARIES

The changed techno-political realities present some fresh challenges to any responsible military leader or diplomat. Firstly, because the past experiences tell us that there is a very fine line between prudent preparation to defend our own assets and provocative military activities that tend to increase the probability of conflict. Secondly, unlike earlier days, the measures of the ultimate success of a military are not only by how well it defeats the enemy but also by how well it is able to provide protection to the growing economy and support the rest of the nation. Therefore, how we ingrain our responses to these demands while forming a cyber strategy would not be as simple as plainly deploying and using the newly discovered cyber weapons. Krepinevech's comments on the issue are quite thought provoking:

> It may, therefore, be difficult for the leadership of one cyber power to determine when, in the mind of its enemy, it has crossed the line between cyber operations that are "acceptable" and those that will trigger a major escalation in the intensity of cyber activity that could lead to catastrophic attacks.

Furthermore, there is always a time lag between the discovery of a new weapon and development of the strategy that would guide its employment and deployment. India became nuclear weapon capable in 1974 with the Pokhran-I test, however, the draft doctrine of credible minimum deterrence came into being only in August 1999.[8] In the absence of a strategy for the employment of a new type of weapon, we run the risk of accidental wars as was seen in the case of the nuclear weapons era. For the first decade or so,

8. http://en.wikipedia.org/wiki/India_and_weapons_of_mass_destruction

post Hiroshima, neither the US nor the erstwhile USSR had a comprehensive strategy for employing (or not employing) nuclear weapons. This resulted in the two superpowers coming to the brink of nuclear war several times, including during the Cuban missile crisis in October 1962.[9] The point driven home is that while there are obvious differences in the nature of cyber war and nuclear war, some experiences highlighting the necessity of a comprehensive strategy are worth contemplating as we develop a strategy for this new type of weapons.

PECULIARITIES OF CYBER DOMAIN

In the domain of kinetic war, one examines the vulnerabilities of the adversary's plans and military hardware, including tanks, airplanes, ships, missiles and other types of vulnerabilities such as the turning radius of a fighter aircraft or the acoustic blind spot of a submarine. Accordingly, specific tactics are developed to exploit these vulnerabilities, and, in some cases, specific weapons are built against them. Also, it is considered less likely for adversaries to be using the same systems as ours, and, thus, vulnerabilities in our opponent's systems are normally different from those of our own. In other words, hardening our own systems against vulnerabilities usually does not impact our ability to exploit the vulnerabilities of an adversary. But in the case of cyber warfare, this equation does not hold good, primarily because the entire cyber domain is built on the foundation of hardware with common processing architectures connected by a standardised system for exchanging data packets across the globe. Added to this basic commonality is the virtual monopoly in operating systems and popular software by Microsoft. As a consequence, at the top level, we share many common cyber vulnerabilities with our adversaries and allies alike. This presents a strategy dilemma for India when developing and using cyber offensive weapons and, at the same time, also trying to strengthen the cyber defences, both of which have become prominent policy concerns.

9. http://www.cbc.ca/news/interactives/tl-cuban-missile-crisis/index.html

STRATEGIC OPTIONS: THE OFFENCE–DEFENCE DYNAMICS

From the offensive perspective, the traditional policy choice would be to classify any vulnerabilities (in hardware, software, or systems) to enable development of exploits and eventually offensive cyber capabilities and also to keep them out of the hands of other states and cyber criminals. This is the traditional choice that governments make when it comes to conducting offensive military campaigns in any domain. Although it can be successfully accomplished in the traditional domains of warfare, in the cyber domain, this choice falsely assumes that only governments are involved in defence and offence. While this is a reasonable assumption in the case of land, sea, or air operations, in the cyber domain, the equations are different for various reasons as given below.

Blurring of Attack Surface

The 'attack surface' is very loosely defined and spread across the military, public and private infrastructure. Vulnerabilities exist in many more places than just operating systems and in many more objects than just traditional desktop and laptop computers. Virtually everything that runs computer software is vulnerable; the newly discovered categories including Programmable Logic Controllers (PLCs) that control the industrial process, Industrial Control Systems (ICS), Supervisory Control And Data Acquisition (SCADA) systems and mobile phone operating systems are receiving increased attention of both the 'black hat' and 'white hat' hacker communities.

Offence–Defence Catch Twenty-Two

There is another hurdle in building already costly cyber defences from our own offensive cyber warriors while planning and executing a covert cyber offensive to permit plausible deniability. This, more often than not, implies that knowledge about such cyber operations would not be shared by organisations and departments even within the same government, making its own systems vulnerable to the same exploits. For instance, a security researcher discovered several new critical ICS vulnerabilities, which he

planned to unveil at a cyber security conference. However, the vulnerabilities he discovered were so serious that he was persuaded by the US Department of Homeland Security and Siemens to forego his talk.[10] Thus, strategies aimed at improving a nation's cyber offensive capabilities would hinder the ability to improve its own cyber defence and result in counter-productive efforts: inter-departmental blame game, and duplication of resources.

For the Indian armed forces and National Technical Research Organisation (NTRO), there would be constant trade-offs between revealing a vulnerability to Computer Emergency Readiness Team (CERT)/ vendors/ industry/ the public so that they can be fixed, and keeping the vulnerability classified so that it can be potentially used offensively by them. This culture leads government agencies to hire experts (similar to cyber criminals) who would dig out the vulnerabilities and develop exploits for cyber offensive operations rather than informing the public or the vendors. This may result in a situation where government agencies and cyber criminals are using the same exploits on our systems at the same time. At an annual hacking contest sponsored by Google in March 2012, a well-known cyber security firm refused to divulge vulnerabilities and exploits that it had discovered in Google's Chrome web browser because it was worth more to it to divulge such information only to its customers, which consist of North Atlantic Treaty Organisation (NATO) governments and NATO partners.[11]

The Cost-Benefit Analysis

The costs of offence, when measured against the combined costs of defence and consequence management reveal some unique trade-offs. On the one hand, attackers seeking to cause damage that will generate strategic effect will require a substantial monetary investment in intelligence, targeting, and testing, and the weapon's shelf-life will be short. On the other, defenders still face formidable costs in protecting infrastructure and conducting

10. Chris Blask, "Network Security: The Threats You Don't See", Infosec Island, June 22, 2011, <www.infosecisland.com/blogview/14682-Network-Security-The-Threats-You-Dont-See.html>.
11. Andy Greenberg, "Meet The Hackers Who Sell Spies the Tools to Crack Your PC (And Get Paid Six-Figure Fees)", *Forbes*, March 21, 2012, <www.forbes.com/sites/andygreenberg/2012/03/21/meet-the-hackers-whosell-spies-the-tools-to-crack-your-pc-and-get-paid-six-figure-fees/>.

consequence management across inter-agency boundaries. Therefore, while it is true that offence is still dominant on one side of the equation, the operational value of weapons is also complicated by their relatively short shelf-lives and some of the uncertainties involved in whether or not they achieve the desired effects on the target.

Investments in cyber defence have a diminishing marginal return per rupee spent on security. Extrapolating from this, the larger the attack surface, the less cost-effective defence is in preventing harmful effects. The diminishing returns on investment in defence relative to offence are especially conspicuous when considering the disparity between "hacking" and "patching" in complexity, cost, and time required. For example, a sophisticated network defence software contains between 5 million and 10 million lines of code, whereas an average attack malware contains an average of 170 lines of code. Also protection of critical government networks typically requires standard government competition and contracting, which can take years before solutions are initiated, whereas designing an attack can be accomplished in weeks.[12] While network defence against sophisticated attackers requires advanced work by highly specialised firms, network attack is literally a cottage industry. This, therefore, calls for the examination of cyber warfare with the same intensity with which nuclear warfare was examined during the Cold War.

Cyber Warfare Strategy Conundrums

The governments that are seeking to both strengthen their own national cyber defences and develop offensive cyber techniques and weapons that can be used against adversaries are faced with a conundrum arising from the unique nature of the cyber domain. Pursuing the usual offence–defence equations in this regard is likely to have an impact outside of the military domain because the same software and hardware is being used across military, commercial and civilian applications. Furthermore, it is very likely that any useful exploits that the armed forces or NTRO discover in

12. David C. Gompert, Phillip C. Saunders, *The Paradox of Power: Sino-American Strategic Restraint* (US: National Defense University, 2011), p. 132.

developing offensive cyber weapons could also be used against their own systems or other government and private institutions, posing a strategy dilemma of either favouring cyber offence or cyber defence.

To understand the development and deployment of cyber weapons, and create the choice between cyber offence and defence, some lessons from the case analyses of the first public demonstration of a cyber weapon, the 'Stuxnet', would serve a good purpose.

CHARACTERISTICS OF A MODERN CYBER WEAPON

The Stuxnet Case Analysis

Originally detected by security researchers in June 2009, the Stuxnet malware was used to target the Iranian nuclear enrichment facility at Natanz. The Stuxnet attacks consisted of multiple versions of a complex Microsoft Windows malware discovered up to mid-2010 with the main target being the centrifuges used at Natanz for enriching uranium. To affect the centrifuges, Stuxnet needed to infect computers known as Industrial Control Systems (ICS) used to programme and control the Programmable Logic Controller (PLC) devices which, in turn, controlled the frequency converter drives that ran the centrifuges.[13] This meant that Stuxnet first needed to exploit vulnerabilities in the host operating system to infect the overall machine, exploit vulnerabilities in the application software for the PLCs, exploit vulnerabilities in the PLCs themselves, and, finally, command the frequency converters in a way that damaged the centrifuges.[14]

Failure of 'Air Gap' Panacea

The first major hurdle in executing the attack was that the ICS computers that Stuxnet needed to infect were not connected directly to the internet. Like the Indian Air Force's (IAF's) Air Force Net (AFNET), the Indian

13. "W32.Stuxnet Dossier", Symantec, ver. 1.4, 2011, <http://securityresponse.symantec.com/en/id/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf>.
14. "Enumerating Stuxnet's Exploits", Langner Communications, June 7, 2011, <www.langner.com/en/2011/06/07/enumerating-stuxnet%E2%80%99s-exploits/>.

Navy's Navy Enterprise Wide Network(NEWN)[15] and the Indian Army's Army Wide Area Network (AWAN), the Iranians had also implemented a common security protocol called "air gapping" (i.e. physical, electrical and electromagnetic isolation) to insulate them from other systems and, in particular, the internet. However, operators still needed a way to update the software on these computers as we update our 'stand-alone' Personal Computers (PCs) and transfer data to and from them. This was done using USB flash drives, which should not have been done. Therefore, the Stuxnet was designed accordingly and was unleashed in three different waves against five different organisations with a presence in Iran.[16] Over a period of time, Stuxnet spread within and between networks until finally it reached the ICS computers, where the payload executed.

Drawing a parallel with the incident, the IAF, Indian Army and Indian Navy operate their computer networks as 'air gapped' from each other and from the internet to ensure network security, however, they have an operational necessity to access and transfer data across multiple networks to achieve their mission. This need, in many cases, puts pressure on combatants to bypass the security features and Standard Operating Procedures (SOPs), thus, promoting the use of devices such as flash drives/ CDs/DVDs between the networks. The IAF has very stringent SOPs for transfer of data between the AFNET and internet; however, incidents of violations keep getting reported.

Advantage Zero Day Exploits

Another observation highlighting the vulnerability of Microsoft Windows monoculture is that Stuxnet took advantage of four zero-day exploits[17] in Windows to infiltrate its targets. The first version of Stuxnet, discovered in June 2009, took advantage of a remote code execution vulnerability in

15. http://articles.janes.com/articles/Janes-Military-Communications/Navy-Enterprise-Wide-Network-NEWN-India.html
16. Ibid., p. 9.
17. Zero-day exploits (actual software that uses a security hole to carry out an attack) are used or shared by attackers before the developer of the target software knows about the vulnerability. http://en.wikipedia.org/wiki/Zero-day_attack

the Windows Print Spooler Service.[18] This vulnerability had been previously disclosed by the security magazine *Hakin*[19] in April 2009, but was not patched by Microsoft until September 2010.[20] Also, a new version of Stuxnet, discovered in March 2010, exploited a previously unknown remote code execution vulnerability in the way Windows handles shortcut or link files.[21] Microsoft issued a security advisory for this vulnerability in July 2010 and a patch to fix it in August 2010.[22] The security firm Symantec privately disclosed two other privilege escalation vulnerabilities to Microsoft as a result of Symantec's analysis of Stuxnet.[23] Probably, Stuxnet's team had discovered these vulnerabilities in Windows and the other parts of the system in the process of development or they had a library of publicly unknown exploits to choose from. Whatever be the case, the more important point is that these vulnerabilities were kept secret and not disclosed to Microsoft. This brings us to the point that the compartmentalisation of cyber offence teams from cyber defence teams is very likely to happen and this would leave many millions of computers owned by governments, companies and private citizens around the world vulnerable to the same exploits, as happened in this case.

Compartmentalisation of cyber offence teams from cyber defence teams is very likely to happen and this would leave many millions of computers owned by governments, companies and private citizens around the world vulnerable.

Minimising Collateral Damage

Another aspect of cyber weapons is their newly acquired ability to restrict collateral damage. Unlike many other types of malware or worm, Stuxnet

18. Ibid., p. 4.
19. Ibid., p. 4.
20. See "Microsoft Security Bulletin MS10-061 - Critical", Microsoft, September 14, 2010, <www.microsoft.com/technet/security/Bulletin/MS10-061.mspx>.
21. "W32.Stuxnet Dossier", n. 13, p. 4.
22. "Microsoft Security Bulletin MS10-046 - Critical", Microsoft, August 2, 2010, <www.microsoft.com/technet/security/bulletin/MS10-046.mspx>.
23. "Updated W32.Stuxnet Dossier is Available", Symantec, updated February 14, 2011, <www.symantec.com/connect/blogs/updated-w32stuxnet-dossier-available>.

took considerable steps to limit its spread as it only spread via USB flash drives and within a Local Area Network (LAN), and each infected device was limited to infecting three others.[24] Stuxnet also contained a code for "self-destruct", and on June 24, 2012, it did so.[25] This indicates the short life span of cyber weapons when compared with kinetic weapons. On the other hand, despite its non-proliferating design, the Stuxnet had infected over 100,000 hosts in 155 countries as of September 2010, highlighting the inherent property of ICT to spread unhindered,[26] albeit the spread occurred because of the still unpatched vulnerabilities in Windows and the widespread carelessness in the use of USB flash drives.

Surgical Strike Capability

Although Stuxnet infected many systems, there is no evidence that it disrupted or damaged any systems outside of Iran. The final analysis of the Stuxnet code has shown that its payload was designed to execute only against specific ICS computers used for the Iranian centrifuges at Natanz. This kind of precision was not seen in earlier versions of cyber weapons. The assigned target for Stuxnet was the Windows machine that was running the Step 7 software used to control the PLC manufactured by Siemens Corporation. To make it more precise, the PLC needed to be a Siemens model 6ES7-315-2 controlling at least 33 frequency converter drives, manufactured by Fararo Paya in Tehran or by Vacon in Finland, running between 807 and 1,210 Hz.[27] This surely requires substantial intelligence gathering, reconnaissance and targeting effort and that is not possible without strong funding support to such operations.

Propagation Dynamics

The reverse engineering effort required to reproduce the cyber weapons is minimal. Once the weapon is released and becomes public, it is possible for

24. "W32.Stuxnet Dossier", n. 13, p. 10.
25. http://news.antiwar.com/2012/06/25/stuxnet-attack-over-as-worm-self-destructs/
26. "W32.Stuxnet Dossier", n. 13, p. 5.
27. Ibid., and Dale G. Peterson, "Langner's Stuxnet Deep Dive S4 Video", *Digital Bond*, January 31, 2012, <www.digitalbond.com/2012/01/31/langners-stuxnet-deep-dive-s4-video/>.

anyone with the tools and motivation to discover how it worked. And, as usually is the case, it takes months to years to patch the vulnerabilities it used, so the hackers take advantage to perpetrate organised crime during this time lag. For instance, Microsoft reported a massive spike in the number of malware infection attempts using the same shortcut/link exploit used by Stuxnet by the end of July 2011.[28] These attempts were especially prevalent in Brazil and the United States, which was not so earlier. Presently, there are other malwares in the wild, known as Duqu and Flame, which bear a striking resemblance to Stuxnet, leading some security researchers to believe they are from the same developers or were built by reusing key parts of Stuxnet.[29] While the *Wall Street Journal* believes that Stuxnet was developed by the Central Intelligence Agency (CIA), with the help of the Department of Energy and Israeli hackers,[30]there are all indications that these have been created by a nation-state.[31]

WHY INDIA SHOULD PURSUE 'OFFENSIVE CYBER WARFARE'

Besides what the Stuxnet analysis shows, there is enough evidence suggesting the lethality of cyber weapons of mass disruption across the globe. In 1997, a teenager shut down air and ground communication at a US airport in Massachusetts, and in 2000, the Russian government announced that hackers had succeeded in taking control of the world's largest natural gas pipeline network, Gazprom, by using a type of Trojan. In 2000, Vitek Boden took control of a sewage pumping station in Australia. He remotely triggered the release of a million litres of sewage into public waterways.[32] Computers and manuals seized in Al Qaeda training camps contained large

28. Holly Stewart, "Stuxnet, Malicious .LNKs, ... and Then There was Sality", Microsoft Makware Protection Centre, July 30, 2010, <http://blogs.technet.com/b/mmpc/archive/2010/07/30/stuxnet-malicious-lnks-andthen-there-was-sality.aspx>.
29. "W32.Duqu", Symantec, ver. 1.4, November 23, 2011, <www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf>.
30. http://online.wsj.com/article/SB10001424052702304821304577440703810436564.html?mod=googlenews_wsj
31. Dr Hamadoun Toure, head of the UN telecommunications agency, told the BBC. *Huffington Post* UK | By Michael Rundle Posted: 07/06/2012 17:04 Updated: 07/06/2012 17:26.
32. Garry Barker, "Cyber Terrorism a Mouse-Click Away" *The Age*, July 8, 2002. http://www.theage.com.au/articles/2002/07/07/1025667089019.html

Offensive cyber warfare as a means of strategic balancing is based on the basic premise that cyber warfare is capable of causing massive damage with little funding, it is difficult to detect and defend against, it provides a high level of deniability, and it eliminates the problem of geographical distance.

amounts of SCADA[33] information related to dams and critical infrastructure. In 2003, the Slammer Worm took a US nuclear power plant's safety monitoring system offline, and the Blaster Worm was connected with a massive blackout in the eastern US.[34] Of late, the world also witnessed the rising level of sophistication, lethality and precision in the modern cyber weapons in the form of Stuxnet[35], Duqu[36], Flame, etc.

The reason why India should pursue offensive cyber warfare as a means of strategic balancing is based on the basic premise that cyber warfare is capable of causing massive damage with little funding, it is difficult to detect and defend against, it provides a high level of deniability, and it eliminates the problem of geographical distance. An offensive approach to cyber warfare is a favourable option considering India's prowess (though not fully oriented towards warfare!) in this domain. By developing offensive capability, India would be able to mitigate if not neutralise the asymmetries of China's Anti-Satellite (ASAT) capability, or its Electro-Magnetic Pulse (EMP) capability. While India, China and Pakistan are nuclear weapon states, the human rights and environmental concerns have relegated these weapons to the role of deterrent, resulting in the emergence of limited warfare. By using cyber warfare, India could achieve the same asymmetric destructive power, while bypassing the drawbacks.

33. SCADA stands for Supervisory Control and Data Acquisition. It generally refers to an industrial control system: a computer system monitoring and controlling a process. The process can be industrial, infrastructure or facility-based as Industrial processes, infrastructure processes or facility processes. http://en.wikipedia.org/wiki/SCADA
34. David Maynor, and Robert Graham. "SCADA Security and Terrorism: We're Not Crying Wolf," *X force, Internet Security Systems*, 2006 http://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf.
35. http://www.virusbtn.com/conference/vb2010/abstracts/LastMinute7.xml
36. http://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf

Offensive Cyber Warfare to Counter China's ASAT

ASAT is being considered as an emerging threat to space-based assets. India's technology and capability gap on this account could be bridged by leveraging cyber warfare capabilities till such time it acquires such capabilities. **Cyber warfare enables effecting far more devastating attacks on satellites by knocking out the corresponding relay stations on earth.** India's focus should be to on neutralising the uplinks and downlinks of the space-based systems of adversaries through diverse forms of cyber attack including the simple Denial of Services (DoS) attack. This would give India the advantages of deniability and low cost. It would also remove distance from the equation, allowing multiple targets to be taken out simultaneously, regardless of location, and it would remove international condemnation and/or involvement.

On the other hand, the use of kinetic kill weaponry, such as China's direct ascent ASAT to disrupt space-based assets has many disadvantages. Firstly, while India's Indian Regional Navigational Satellite System (IRNSS[37]) that would provide surveillance, tactical communication and precision navigation makes it a desirable target, the attack surface would not be limited to a single satellite; rather, it would be a constellation of seven satellites. When one is destroyed, others can be manoeuvred to fill holes in the net. Secondly, at any given time, not all of these satellites are within striking range. This means a sky clearing operation would take a significant amount of time, thereby revealing Beijing's intentions. Thirdly, it would risk retaliation and international pressure, putting China at a disadvantage and, finally, there is no guarantee that such an attempt would be successful, as each launch requires precise targeting, and China's ASAT has only been tested once.

Cyber Offensive as an Alternative to Nukes

Going purely on the capability basis, India could destroy a vast majority of China's electronics, including computers, cars, phones, and the power

37. http://en.wikipedia.org/wiki/IRNSS-1'the IRNSS-1 expected to be launched on board PSLV-HP by May/June 2013'

grid, using an EMP burst through high altitude nuclear explosions with as few as three nuclear bombs, like any other nuclear armed state could, and against Pakistan the effort required would be much less. In fact, it is now public that the US, China, France, and Russia all are using an EMP burst as a surprise first strike in war-games, as reported by numerous sources.[38] However, such brute-force tactics would cause international outrage as an EMP burst violates an international treaty, it damages the environment, and it indiscriminately disrupts everything in its blast radius. Alternatively, shutting down China's power grid, production lines, water utilities, chemical plants, telecommunications, and transportation routes is possible through cyber attack, and it would provide the benefit of deniability also.

Offensive Cyber Warfare for Technology Leapfrog

ICT is a key enabler for the developed countries; for emerging nations like India, it offers a great possibility to leapfrog many competitors, and for those still in the agricultural age, it offers the ability to conduct asymmetric operations.[39] Espionage and technology transfer prosper in cyber warfare, where being physically present is not required, and attribution becomes increasingly difficult. Although it does not fall strictly in line with India's non-coercive and rather submissive approach to security strategy, cyber warfare allows acquisition of foreign military knowledge, to quickly catch up and begin working at a comparable level, rather than investing large amounts of time and effort to acquire this knowledge independently. While India has been subjected to large scale and complex espionage operations, involving exfiltration of thousands of classified and sensitive government

38 Hearing on "China's Proliferation Practices, and the Development of its Cyber and Space Warfare Capabilities" Tuesday, May 20, 2008, Room 562, Dirksen Senate Office Building First Street and Constitution Avenue, NE Washington, DC 20510. http://www.uscc.gov/hearings/2008hearings/agenda/08_05_20agenda.pdf; Liang Qiao and Xiangsui Wang. *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, February 1999). http://www.terrorism.com/documents/TRC-Analysis/unrestricted.pdf; Bartlett, Roscoe. "Nuclear Electromagnetic Pulse", *US Congressional Record*, June 9, 2005. http://cryptome.org/bartlett-060905.txt www.icnnd.org/research/New_Weapons_Technology.pdf

39. Jason Andress and Stev Winterfeld, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners* (Elsevier Inc, 2011), ch 1, p. 9.

documents[40], **it is about time to extrapolate Chanakya's idea of having a great deal of emphasis on spies, grouped into a separate organisation directly reporting to the king,**[41] **in the cyber domain.**

As an empirical observation of international politics, the nation-states with a proven history of cyber espionage do not necessarily attract sanctions or get subjected to international pressures as long as they are able to propel their economy and enhance the interdependence of the world economy. The case in point is China, where in spite of evidence of mass exfiltration of Research and Development (R&D) data, political intelligence and intellectual property from the EU, US and India by online espionage activities, Europe still supplies technology to China, and the EU has a regular dialogue with China.[42]

Offensive Cyber Warfare for Power Projection

India currently lacks the cyber power projection to protect its National Critical Information Infrastructure (NCII) from disruption. Online technology transfer and the further development of Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) are crucial to extend this power projection. Online Psychological Operations (PSYOPS) and media warfare would also enhance India's soft power.

Offensive Cyber Warfare to get Military and Financial Edge

In 1991, having faced the balance of payment crisis, India opened the doors to the new neo-liberal policies, including opening for international trade and investment, deregulation, initiation of privatisation, tax reforms, and inflation-controlling measures. Since then, it has seen a sustainable economic growth. Economic growth is critical to military development;

40. Wing Cdr M.K. Sharma,*Cyber Warfare: The Power of the Unseen* (New Delhi: KW Publishers, 2011) ch. 6, pp.192-199.
41. Wing Cdr (Dr) R. Venkataraman Ph.D, *India's Higher Defence: Organisation and Management* (New Delhi: KW Publishers), ch. 1, p. 15.
42. Pieter D. Wezman and Matieu Gilles Duchatel, " CAPS-SIPRI Roundtable Discussion", Centre for Air Power Studies, New Delhi, March 20, 2013.

The information revolution has given more power to individuals and increased globalisation through the interconnectedness of economies, rapid dissemination of news, and improved access to communication and information of all types.

economic growth creates a greater energy demand, which, in turn, creates a greater military demand, thus, the two form a positive feedback loop,[43] of which India should take full advantage.

The information revolution has given more power to individuals and increased globalisation through the interconnectedness of economies, rapid dissemination of news, and improved access to communication and information of all types. To compete on a global level without the use of these technologies would place India at a significant military and economic disadvantage. For this reason, the benefits of economies becoming electronically reliant outweigh the risks involved, and it is imperative for any growing economy to embrace this technology. Therefore, to benefit from the positive feedback loop of economic growth and military development, India must be able to guard its assets against cyber attacks. Further, it is impossible for a nation to develop a defence against cyber warfare without simultaneously learning how to execute attacks itself.

IN THE DEFENCE OF 'CYBER DEFENCE'

The main objective of our national security policy is the defence of the sovereignty and integrity of India. Thus, we develop/procure weapons primarily to safeguard the nation and not for extending our hegemony over various domains such as land, sea, air space and cyber space. While this seems quite logical, there are those who would profess that the best form of defence is offence. They believe that the capability of destroying the enemy by an preemptive attack would outweigh the requirement for a defensive strategy. This approach has proved to be dangerous and costly to

43 John G. Ikenberry,. "The Rise of China and the Future of the West", *Foreign Affairs* , January/ February 2008. http://www.foreignaffairs.org/20080101faessay87102-p0/gjohn-ikenberry/ the-rise-of-china-and-the-future-of-the-west.html.

many nations in the history of warfare. In the 1950s, the US Air Force Gen Curtis LeMay as Commander of the Strategic Air Command convinced RAND Corporation analysts that his bombers would not be destroyed on the ground by a Soviet attack because "we are going first". Another strategic fallout of the same argument was when the Bush Administration justified post 9/11 that it would be too expensive to defend the US against a terrorist attack at home so "we need to go out to the source"[44]. Hence, the global war on terror that burdened the US with two wars over a decade, over US$ 2.4 trillion and, of course, the loss of more than 5,000 American lives.

The capability of destroying the enemy by an preemptive attack would outweigh the requirement for a defensive strategy.

In the cyber domain, there are a few compelling factors for India that make a strong case for a defensive strategy, at least for the coming decade. Firstly, India's gaping vulnerabilities because of the growing dependence of its National Critical Infrastructure (NCI) on ICT with no comprehensive national cyber defences. This needs to be seen in the light of recent incidents of Chinese exfiltration of sensitive government data and the possibility of them helping Pakistan to provide highly capable hackers in the future. Secondly, the comparative importance of defences could be argued on the premise that even if our cyber offensive capability is able to disrupt/ degrade/ manipulate / corrupt the enemy Air Defence (AD) network/ banks/financial institutions, etc but our NCI is under attack [say the Bombay Stock Exchange / National Stock Exchange (BSE/NSE) is put down or the data therein is manipulated or the banking system is degraded for weeks together], the cost of such loss of faith of the populace in the system and the inconvenience would have a far more grave effect on democratic India than it would have on, say, the Chinese government for a similar attack on them. Thirdly, increased vulnerabilities to cyber attack lead to self-deterrence and, thus, likely reluctance to use even our superior conventional weapons in a conflict situation. Fourthly, **with our undefended NCI under attack, we**

44. Clark and Knake, n. 3, ch. 5,.p. 158.

would be forced to escalate in a cyber conflict very quickly. We would need to be more aggressive in knocking down enemy information systems to prevent further damage to our NCI. Fifthly, unlike a conventional offensive, in the cyber domain, you cannot destroy all the enemy's offensive capability, as the cyber weapons may already be in Indian cyber space and just need a trigger. Finally, lack of cyber defences could widen the already existing strategic power imbalance between India and China.

For example, if China is able to demonstrate that it can exploit the vulnerabilities of India's NCI, implying the possibility of greater damage, it would increase the credibility of China not only in the India-China military calculus but also in the US-China military, economic and political balance. Ironically, in such a scenario, a higher level of cyber attack capability is not likely to improve the imbalance in favour of India. Therefore, to reduce the risk of any nation threatening to use cyber weapons against it in a crisis, India must have credible cyber defences. Having assured defence, India should be able to deter its adversaries on the basis of offensive cyber warfare capabilities so developed based on broad-based technical Intelligence, Surveillance, Reconnaissance (ISR) and precise targeting of the potential adversary's NCI 'attack surface' spread over both civil and military cyber space.

Cooperation and Coordination Compulsion

Increased cooperation and coordination among and within nation-states—amongst the armed forces, private industry and academia—forms a significant element of cyber defence. Today, the private sector represents a significant part of the NCI attack surface which is required to be protected. Many computer systems of the NCI widely use commercial software applications and architectures, thus, making the protection of NCI partly reliant on discovering and fixing of vulnerabilities in commercial software.

Academics already play a significant role in the cyber security world, but efforts by researchers are often hindered by corporations and governments

because they are seen as a threat and not an asset.[45] This would need to change, and the cyber community would need to adopt a favourable attitude towards any research and experimentation that leads to a better understanding of cyber vulnerabilities and weaknesses in security architectures. The public is often overlooked but plays a potentially significant role in cyber defence. The many millions of personal computers are potential weapons that can be compromised by an attacker and turned into weapons, for example, as part of a botnet running a denial of service attack. Compromised personal computers, mobile devices or online accounts of government officials and corporate executives could provide critical information that leads to the compromise of protected systems. Friends and relatives on social networks are also potential avenues of attack, potentially more likely to succeed because of their trusting nature.

Thus, policies aimed at improving a nation's cyber defence would necessarily need to increase the amount of information-sharing among governments, industry, academia and potentially even the public, and make major changes in the current classification policy for cyber vulnerabilities and attacks. Governments, industry and academia would need to share information about the latest attacks, malware signatures and vulnerabilities.[46] Incentive programmes for the responsible disclosure of vulnerabilities, such as those already being run by Google and the Mozilla Foundation for their respective web browsers,[47] could greatly increase the number of people looking for vulnerabilities and the rate at which they are discovered and fixed. However, these approaches would also have an increasingly negative impact on the ability of a state to develop and field offensive cyber capabilities over time, largely through the increased cost

45. Jaikumar Vijayan, "Carrier IQ Drops Legal Threat Against Security Researcher", Computerworld, November 28, 2011, <www.computerworld.com/s/article/9222203/Carrier_IQ_drops_legal_threat_against_security_researcher>.
46. Jason Healey, "Cybersecurity Legislation Should Force U.S. Government to Listen Less and Speak More", *The Atlantic*, March 15, 2012, <www.theatlantic.com/technology/archive/2012/03/cybersecurity-legislationshould-force-us-government-to-listen-less-and-speak-more/254491/>.
47. "Encouraging More Chromium Security Research", The Chromium Blog, January 28, 2010, <http://blog. chromium.org/2010/01/encouraging-more-chromium-security.html>; and "Bug Bounty Program", Mozilla, February 1, 2012, <www.mozilla.org/security/bug-bounty.html>.

of finding new vulnerabilities and developing offensive weapons against them even as they are being patched.

CYBER DETERRENCE: IS IT WORTH IT?

Learning from the previous wars and extrapolating this knowledge to the realm of cyber space, cyber deterrence seems to be the natural good idea like missile deterrence and nuclear deterrence proved to be effective strategy in the past.[48] But, the peculiarity of cyber attacks is that they are enabled not through the generation of force but by the exploitation of the enemy's vulnerabilities. Permanent effects are hard to produce unlike traditional military action through conventional or unconventional means. So is it fair to draw a direct analogy between nuclear deterrence or traditional military deterrence and cyber deterrence wherein we may not know exactly who did it? Or what is the assessment of collateral damage due to interdependence on target infrastructure? Or how much are we prepared to absorb of a retaliatory cyber attack?

Another difference in the notion of deterrence in cyber space is that something that works today may not work tomorrow (indeed, precisely because it did work today). Thus, deterrence and war-fighting tenets established in other media do not necessarily translate reliably into cyber space. Such tenets must be rethought.

Cyber Deterrence: The Attraction

The attraction of cyber deterrence is that, if it works, it can reduce the cost of defending systems. Instead of having to put money into making systems more secure, the defender inhibits the attacker's efforts by threatening retaliation against successful attacks.[49] So if an attacker can be persuaded to reduce its efforts in the face of punishment, the money thus saved by the defender that would have been spent on the security (to achieve the same level of assurance) is worth considering.

48. During the Cold War, the nuclear stand-off between the US and Soviet Union never went out of control. This provides the historical basis for believing that cyber deterrence should work.
49. Martin C. Libicky, *Cyber Deterrence and Cyberwar* (RAND Project Air Force,2009), ch.3, p. 42.

As with any other type of deterrence, the aim of cyber deterrence would be to reduce the risk of cyber attacks to an acceptable level and at an acceptable cost. And if this aim could be achieved through cyber security measures alone, then why build cyber deterrence systems at an additional cost? The problem with cyber security is that there is nothing like total security and near total security too may be achieved at prohibitive costs. For instance, the expenditure of US organisations on information security easily measures in tens of billions of dollars a year yet security breaches occur daily.[50] This is why the US President's budget request allots more than $13 billion to cyber programmes, nearly 16 percent of a federal Information Technology (IT) budget totalling about $82 billion.[51]Therefore, cyber deterrence becomes an absolute necessity.

Cyber Deterrence for Buying Time

India seeks to maintain domestic and regional stability while developing its economic, military, technologic, scientific, and soft power. It also seeks a balance between military and economic development, believing they are mutually dependent. At this juncture, while India tries to equitably match its military power with China, it could buy time by keeping a low profile and depending on cyber reconnaissance. Cataloguing adversary weaknesses not only provides an asymmetric advantage in the event of a conflict, it also acts as a deterrent while India catches up with its military modernisation drive.

Cyber Posturing: A Potent Foreign Policy Instrument

For India, cyber posturing could be a potent foreign policy instrument. **Unlike conventional military deterrence, in cyber space, the acquired offensive capabilities do not necessarily have to reside in military organisations**. India's prowess in IT and IT Enabled Services (ITES)

50. Dawn S. Onley, "Army Urged to Step Up IT Security Focus," *Government Computer News*, vol. 1, no. 1, September 2, 2004.
51. http://www.washingtonpost.com/business/on-it/obamas-budget-proposal-would-increase-spending-on-cybersecurity/2013/04/14/218e71d6-a2b8-11e2-be47-b44febada3a8_story.html

Cyber warfare strategy would include India's take on employing cyber offensive, building up cyber defences and conveying cyber deterrence power to the adversaries.

could be leveraged to build cyber deterrence capabilities to gain asymmetric advantage against militarily mightier potential adversaries. Here, the concept of employing week-end cyber warriors on cyber warfare projects is worth considering.

STRATEGY OPTIONS FOR INDIA

Cyber warfare strategy would include India's take on employing cyber offensive, building up cyber defences and conveying cyber deterrence power to the adversaries. This would be supported by a cyber security strategy to enable cyber capability building that remains at the core of the issue. Towards this, cyber security strategies proposed to be adopted during the Twelfth Five-Year Plan include:

- Enhancing the understanding with respect to factors such as dynamically changing threat landscape, technical complexity of cyber space and availability of skilled resources in the area of cyber security,
- Focus on proactive and collaborative actions in public-private partnership.
- Enhancing awareness and upgrading the skills, capabilities and infrastructure.
- Improving interaction and engagement with various key stakeholders.
- Carrying out periodic cyber security mock drills to assess the preparedness of critical sector organisations to resist cyber attacks and improve the security posture.
- Supporting and facilitating basic research, technology demonstration, proof of concept and testbed projects in thrust areas of cyber security through sponsored projects at recognised R&D institutions.

Six focus areas have been identified for implementation of the cyber security activities. These are: Enabling Legal Framework, Security Policy, Compliance and Assurance, Security R&D, Security Incident – Early Warning and Response, Security Awareness, Skill Development and Training and

Collaboration.[52]

Pursue Cyber Research to Create Cyber Resource

If there could be any single approach that could be called the 'silver bullet' to deal with cyber warfare, it would be to create cyber resources. There is no point in crafting a strategy without having resources in that domain. Cyber research is the key to creating resources in all cyber sub-domains such as cyber power, cyber space, cyber strategy, institutional issues, cyber assessment and cyber policy.

- *Cyber power research* needs to, firstly, adequately assess the relative worth of cyber assets in the political, economic and social levers of national power. Secondly, at the military level, it is important to not only focus on the benefits of cyber power but also to carry out military risk assessment of relying on cyber space. This would require development of intellectual capability, methodology, tools and data collection. Lastly, the armed forces are required to quantify the future cyber conflict scenario with potential adversaries.
- *Cyber space research* is aimed at identifying and projecting the future technologies that have the potential of substantially altering the performance of the cyber space. Working on such technologies/ architectures would provide technology leadership to India while providing better protection to essential data in cyber space.
- *Cyber strategy research* would deal with challenges posed by various entities/actors that are cyber empowered. This would deal with the vital questions of adopting cyber offence, cyber defence or cyber deterrence approaches. Research is also required to investigate the feasibility of collective development of 'tailored cyber deterrence' say by the BRICS (Brazil, Russia, India, China and South Africa) nations, firstly, to create common understanding and interdependence and, secondly, to communicate such a concept to potential adversaries.

52. N. Sitaram, Distinguished Scientist & Former CC (R&D), DRDO, Twelfth Five-Year Plan (2012 – 17) Information Technology Sector, Government of India Ministry of Communications & Information Technology, Department of Information Technology, p. 4.

Cyber assessment research is needed to upgrade from rudimentary ways of cyber power assessment to developing analytical methods and tools for more objective and realistic assessment of our own and the adversary's cyber power.

- *Institutional issues research* is required to bridge critical gaps in the areas of internet regulation, e-governance, information sharing architecture, and legal issues. The ICT infrastructure must be regarded as an 'ecosystem' in which everything is interconnected. It functions as a whole; it must be defended as a whole.[53]
- *Cyber assessment research* is needed to upgrade from rudimentary ways of cyber power assessment to developing analytical methods and tools for more objective and realistic assessment of our own and the adversary's cyber power. This obviously demands huge intellectual capital to address the issues of cyber infrastructure and cyber strategy.
- *Cyber policy research* would iron out many contentious issues related to major policy, including the legal framework, e-governance and international cooperation on information sharing, etc.

Cyber Reconnaissance: A Strategic Tool

Cyber reconnaissance appears to be the most beneficial tool of cyber warfare. Beyond finding exploitation points in the attack surface of adversaries for future attacks, the commercial sector allows India the opportunity to skip generations of research and development efforts, levelling the playing field in science and technology, and boosting economic and military might. This boundaryless military operation, could provide access to the mind of the enemy on any issue, including how he thinks on human rights issues in relation to soft power, globalisation, international condemnation, and the legal apparatus.

The relative ease with which the Titan Rain attacks were conducted makes the private sector computer networks look like an easy target.[54]

53. Toomas Hendrik Ilves, President of Estonia, "Cyber Security: A View from the Front", *International Herald Tribune*, April 12, 2013.
54. Marcelo Almeida, "Cyberwar: The Beginning" *Rand Corporation Monograph*, July 2006.http://www.rand.org/pubs/monograph_reports/2005/MR580.pdf. http://www.zone-h.org/index.php?option=com_content&task=view&id=13932& Itemid=30&msgid=710.

While the government and defence installations are heavily funded for security, the private sector is not. Many of these systems do not support authentication, encryption, or basic validation protocols; of those that do, most run with security features disabled. The vulnerability of the private sector's computer network, due to a lack of understanding or a lack of incentive, provides India with the opportunity to cripple the adversary's civil information infrastructure.

For instance, Hugo Teso a security consultant at n.run, Germany, demonstrated that one could manipulate the steering of a Boeing jet in auto pilot mode, make oxygen masks drop down and even cause the plane to crash by setting it on a collision course with another plane.[55] Firstly, the Automated Dependent Surveillance Broadcast (ADS-B) which is a surveillance technology used for tracking the aircraft is unencrypted and unauthenticated and has no cyber security. Secondly, the Aircraft Communication Addressing and Reporting System (ACARS) which is used for exchanging messages between the aircraft and stations via radio or satellite also has no security features.

Increase Hardware and Software Market Share

India should seek to gain a market share in the production of ICT software and hardware as a means of increasing its cyber warfare capability. On the infrastructure level, India could seek to increase ownership of submarine cable infrastructure, allowing it further access to cyber reconnaissance or the option of shutting down portions of internet connectivity during times of war.

Build Espionage Backbone

India must also grow in the field of microchips, something that other countries need for defence related electronics. Not necessarily for embedding exploits, but dominance in this field would give India access to critical individuals and information through partnership, come close to sensitive information and hardware when needed and conduct social engineering or Human Intelligence (HUMINT). Fears of international pressures or

55. Sophie Warnes, "Control an Aircraft with an Android Phone", *The Times of India*, April 14, 2013.

sanctions for adopting this approach, as some would believe, may not be well placed. Empirically, for instance, despite ample clear indications of many cyber espionage operations to exfiltrate R&D, design and political sensitive data on a large scale from all over the world, including the EU countries, US and Asian nations, China continues to have improved trade relations and technology transfer agreements with the EU and US. The key here seems to be creation of economic interdependence.

CONCLUSION

As a starting point to deal with the cyber challenges, India should take concurrent steps at the strategic, operational and tactical levels. The strategic level approach must be based on building strong defences ensuring resilience of the National Critical Infrastructure (NCI). At the operational level, we must develop credible cyber offensive capability employed in rigorous in-house experimentation, simulation and exercises that would be deployed against a highly advanced cyber adversary. Lastly, the tactical level actions would look into the mission oriented approach to influence military operations that would integrate the physical, information, social and cognitive domains together to execute Net-Centric Operations (NCO).

In essence, while we develop a national strategy on cyber warfare, we must create cyber resources and procedures simultaneously that would contribute towards achievement of specific national security objectives. Those resources would be technological, organisational and human, employed for cyber offence, cyber defence, cyber deterrence or combinations of these. **Without the creation of cyber resources, the cyber strategy is like having an air strategy without having aeroplanes**. The strategy must be based on partnership given the inseparability of private, government and military cyber space. The armed forces are becoming increasingly dependent on the private sector for development, maintenance and security of national cyber space capabilities. In many ways, we are facing something more like the Cold War where cyber espionage and spending on cyber warfare are the missiles that will determine the outcome of future conflicts.