Cyber Threat and Military Challenges*

Brigadier Abhimanyu Ghosh (Retd)**

Introduction

History has shown that wars are won not only by the courage and strength of the men and women on the battlefield; but also, by the evolving technology adopted by the military. In the cyberspace, two distinct regimes emerge for the military. The *first* regime is the open network with its inherent risks and vulnerabilities which is essential for collaboration, information sharing, logistics etc. The *second* regime of closed network meets the demands of security, speed of operation and availability of information at the right time and place. To maintain confidentiality, integrity and availability, closed network is air gapped from open network. In addition to these networks, the military is also exposed to commercial off the shelf (COTS) hardware and software products for wireless, cellular phones, computers, networking equipment etc. Therefore, increased dependence of the military on civilian cyberspace capabilities have inherent risks and make them vulnerable to cyber-attacks by attack vectors which are prevalent in commercial/open cyberspace. This paper draws attention to current cyber threats and challenges that the military faces.

Cyberspace

Cyberspace includes not only the internet but also telecommunications, cellular phone technologies and wireless data services. The technologies involved, such as bandwidth, interoperability, processor speed, functionality and security vulnerabilities have evolved over time.

Design Flaw. Internet which is the major platform in cyberspace is loosely based on the legacy model of Open System Interconnection (OSI) in which most commonly, internet protocol (IP) is paired with Transmission Control Protocol (TCP) to form TCP/IP. The three way handshake of the TCP software for packet exchange is user-friendly but is one of the causes of flooding and other attacks.

SCADA. Increasingly today, supervisory control and data acquisition (SCADA) devices are being used to control the logical processes in the industry and weapon systems. These are designed to maintain isolation in the cyberspace. However, the need for remote access for management by a private/public network introduces significant dependency of the SCADA devices to other elements of cyberspace.

Data. Cyberspace is also about its contents / data in storage, transmission and processing. Preserving the confidentiality and integrity of data is of concern to the Military.

Social Networking. The discussion on cyberspace is not complete without the man-made digital world created to gain access to information and share it between people and machines. With the ever increasing popularity for on-line communities, blogs, social networking, cyberspace is having an increasing impact on the economy, society and national security. Recent events in North Africa, Middle East and even the Wall Street protests are pointers to the phenomenon.

Threat Scenario

Today, every nation with a reasonable employment of Information and Communication Technology (ICT) is a victim of cyber attack. The long list of victims, according to a report by the security company McAfee, include the governments of the USA, Taiwan, India, South Korea, Vietnam and Canada among others. In the case of United Nations, according to the report the hackers broke into the computer system of its Secretariat in Geneva in 2008, hid there for nearly two years and spied through secret data. Added to these are the recent headline grabbing hacks, such as on Lockheed Martin, the International Monetary Fund, Citigroup, Sony Corporation; and RSA, the security division of Enterprise Strategy Group (EMC) etc. Such attacks have continued for more than five years. Added to these are the cyber attacks which are employed in coordination with kinetic attacks, to act as force multiplier or as a tool to effect cyber espionage and for massive scanning and mapping of adversary's assets of information in cyberspace. Currently attackers are able to exploit all the advantages of operating on the internet including operational agility, massive force multiplication and rapid development of attack to exploit newly discovered vulnerabilities. A factor fuelling growth of cyber attacks is bot (ROBOT) software. Bot controlled machines give attackers economies of scale in launching attack and allow them to set-up virtual super computer that could rival the computer power of a nation state. Bots can conduct massive flooding, crack crypto-keys or mine sensitive data. The interchangeable modular software in a bot offers an attacker to maintain flexibility and deniability. Attackers also increasingly rely on polymorphic codes to evade signature based detection tools. The 'moving target' of code make analysis by defenders more difficult. Because of the spread of the bot network, the attack typically comes simultaneously from multiple countries often fuelling trust deficit among friendly countries. Significant threats emanating from embedded systems in imported equipment call for stringent standards and certification. Supply chain threats emerge right from the design stage to development and finally in its deployment.

Players in Cyberspace

The cyber warfare is a unique domain, unlike other military domain when the players are limited. In every other domain, military had the exclusive preserve of its weaponisation and security. However, in this man-made domain, both the adversary and defender share the same virtual territory. A hacker coexists in the same network as the critical infrastructure and is very difficult to identify. The various types of players are :

(a) **Individual Players.** Increase in sophistication of cyber attack tools and automated deployment enable even individual players to attack and cause significant damages to an organisation/state. The word 'hacker' at once brings to mind a person who is socially dysfunctional, brilliant at software programming and with a desire to save mankind. That would be true, but now there are enough individual varieties to merit a zoology-like classification - White Hat, Grey Hat, Black Hat, Script Kiddies, Mules, Herders and so on.

(b) **Hacktivists.** In contrast to individual geeks, these loosely organised group of hackers come together to attack a nation/organisation for a cause and ideology. More important than the individual skills are their affiliations. At the top are the hackers with political belief. They are the *Brahmins* of the hacker world. The most famous of such groups is Anonymous which, ironically, uses hacker attacks to force governments and corporations to become more transparent. It was Anonymous that attacked the websites of Visa and MasterCard when they stopped accepting donations meant for Wikileaks' Julian Assange.

(c) **Cyber Criminals.** Cyber criminals are much more organised today rather than in the past and have a parallel economy running underground. Business process are getting sophisticated and resemble major economic model in real world with service providers, middlemen and consumers. Rival business are controlling bot networks along with Mules and Herders and command and control services.

(d) **Cyber Terrorists.** Terrorists significantly leverage the internet to carry out their activities such as communication, propaganda, recruitment and other activities. The digital revolution and easy availability of technology has unleashed non state actors and individuals to control, occupy and operate in cyber territory. This creates new power asymmetry and magnifies their clouts.

(e) **Non-State Actors.** These players may or may not have an affiliation with the Government. But today, they play a significant role in making the cyberspace insecure and bring international communities in a huddle to bring them to book.

(f) **State** The asymmetry in conventional arms as also asymmetry in internet penetration are driving some of the less developed countries to adopt clandestine operations to set-up offensive projects in the cyberspace. Non attributability and deniability are causes of worry.

Targets

The range of targets vary from individuals to nation states:-

(a) **Individuals.** Individual data such as personal, business and financial information is being stolen for various purposes such as impersonation and financial fraud.

(b) **Individual Organisations.** Business secrets, intellectual property and personal information of employers are being targeted.

(c) **Nation States**. The individual nations are experiencing cyber attacks on their critical infrastructure which lead to leakage of state secrets and compromising SCADA systems etc. Espionage and data theft are the prime motives of an attacker during peace time. Such actions could lead to military intervention also.

Military Challenges

As the cyberspace is all pervading and touches each and every aspect of life, it is very difficult to categorise the challenges as military or otherwise. Some believe that an attack on economic infrastructure could constitute an act similar to that of war, as today it can impact the national security. The entire spectrum of attack, from the scanning of network to cyber-crime espionage and finally the full scale cyber attack, need to be studied to draw the distinction. The major challenges to the military are:-

(a) **Classification as an Act of War.** The biggest challenge that the military faces today is to identify "an act of war". During the Distributed Denial of service (DDoS) attack on Estonia, while one country was suspected of launching the attack, more than 17 per cent of DDoS traffic originated from another country. Can this be taken as an act of war by either of them? Also, even if the nation state is not directly involved, such actions by a single person/group of person may be recognised as hostile action by the affected country, e.g. pulling down nuclear installation causing an accident and stealing critical information. Would such acts automatically imply that a country has started the war? The question answers: what constitutes cyber war? Can attacks on critical infrastructure owned by private sector, which also support humanitarian activities, be used to achieve military objectives and recognised as aggression? Legitimate cyber soldiers are indistinguishable from script kiddies. Therefore, should they be treated as non-combatants? Again, how does one know if third parties are acting on behalf of a nation state. When does cyber espionage graduate to a cyber-war? How do the Geneva and Hague conventions get corelated in the cyberspace? All these questions pose a major challenge to the military, which has to effectively defend the nation's sovereignty in cyberspace.

(b) **Attributability.** Nowhere in any domain, except in cyberspace, it is easy to remain "anonymous". It is very difficult to attribute a hostile act to a nation/individual player, when lethal attacks, such as DDoS attacks are launched. Attribution to a state is easy but, it is more difficult to pinpoint responsibility in case of non-state actors. Often, the country of origin of the attack turns out to be neutral player and the hostile actor is never identified to facilitate conviction. Even in the case of DDoS against various countries and the recent StuxNet attack, the act of warfare in cyber domain could not be clearly attributed. Thus attribution problem marks an important distinction between cyber warfare and traditional warfare regarding intent and identity, which are not revealed clearly.

(c) **Maintenance of airgap**. The military strives to maintain airgaps between its sensitive network and open network. However, the need for updation of software, upgradation, transfer of data/software between the classified and unclassified system etc. often pose a threat to the entire military system.

(d) **Policy Compliance.** People, process and technology are the three pillars to maintain cyber security. However, in spite of the technology and the policy for implementation, the processes incorporating the best practices are often ignored due to lack of awareness and the auditors lacking teeth to ensure policy compliance.

(e) **Protection of SCADA system.** It is in the news that probably the StuxNet was introduced by way of insertion of a thumb-drive containing the malware on to the classified system. How does that happen? The internal threat by way of a prepositioned human mole or simply an ignorant and unaccountable user could jeopardise the security of the 'SCADA' system.

Weaponising Cyberspace

Even though, the term "Cyber Warfare" has been used for more than two decades, it was only recently that the world saw StuxNet. StuxNet employed no fewer than 'four zero' – day vulnerabilities and demonstrated deep knowledge of the inner working of the SCADA. This shows very clearly that weaponising the Cyber Warfare is very complex involving detailed planning by one or more nation states, non-state actors and private players. A malware specifically affecting only the adversary's network, without any collateral damage to civilian/humanitarian networks that too at the critical time, is still far away before being productionised at a mass level and is a great challenge. It is visualised that future weapon stockpiles will include stashes of zero day vulnerabilities, botnets, control codes and sophisticated malware.

Human Resources

In the rapidly evolving field of cyber operations, it is a major challenge to attract and nurture talent. The shelf life of an expert is very less unless he is exposed to new technologies and concepts. Numerous studies have shown that the military in its present state, tends to get overwhelmed by lack of expertise; unlike the adversaries who exploit the knowledge and expertise of young generation and thus amass faceless hackers in thousands to attack a nation's infrastructure.

Developing Deterrence Capabilities

The evolution of Cyber Operations doctrine is still in its nascent stage. However, some of the strategic documents available in public domain seeking international cooperation are professing deterrents, proportional response and action in self defence. Deterrence must be based on credible assurance of the capability to punish. How does deterrent work when capabilities are secret, weapons undemonstrated and adversary unidentified. With attributability being a major technical challenge cyber offence may not be the best form of cyber defence. Added to these are the challenges posed for adherence to internationally accepted laws of armed conflict and determination of threshold for the military to exercise proportional response.

International Cooperation

Operational stability and security of critical information infrastructure is vital for security of any country. Most countries have adopted comprehensive domestic cyber laws. India, too, has enacted IT Act 2000 (amended in 2008). However, national laws are not sufficient to address global concerns. Thus various international initiatives have been taken at the level of United Nations, ITU, EU and other regional bodies to harmonise domestic laws with international norms. The efforts made by these organisations and more specifically Internet Corporation for assigned Names and Numbers (ICANN). At present, the coordination of cyber domain is de-facto exercised by a few international organisations including ICANN, Internet Engineering Task Force (IETF) etc. for its governance. The root servers are not spread out evenly geographically. The military needs adequate cooperation from these organisations and service providers to address large scale attacks. Efforts for Internet governance by International Telecommunication Union (ITU) World Summit on the Information Society (WSIS), ICANN and some of the other organisations are laudable but at times they act at cross purposes.

The fundamental difference between other domains and cyber domain is that the latter is a borderless domain. Today internet is torn apart by three separate but related forces. The Governments are reasserting their sovereignty, IT companies are constructing and controlling their digital territory while individual owners of data assert their rights to privacy and IPR. Territorial jurisdiction and jurisdiction in cyberspace need to be distinguished. Hence, any initiative for cyber peace and its implementation will succeed only when all stake-holders/nations are involved in framing a consensus. The international community must come together and realise that enormous benefits of internet will be lost if it is used as an instrument of harm outside the rule of law. The nation states must come together to work collectively to harness the power of cyber domain and pledge not to use cyberspace for hostile activities that pose threat to international peace and stability. As far as military domain is concerned, the following aspects need attention of international community:-

(a) **Act of Cyber Warfare.** To quote Clausewitz *"War is continuation of political activity by other means".* Since all / most attacks are not politically motivated, they need not be termed as cyber war. A consensus must be evolved amongst all nations to define the "Act of Cyber War" without expending all other instruments of nation security. All acts, howsoever malevolent need not be hyped to the level of cyber war. Law enforcement agencies and legal instruments of respective nations should play their legitimate roles. Therefore, nation states need to cooperate to de-escalate weaponisation of cyberspace, though proactive defence and technological innovation in cyberspace are a necessity.

(b) **Cooperation Against Cyber Attacks.** Defence against cyber attacks will only be successful, when the countries co-operate and mount a coordinated defence. Recent DDoS attacks, has brought the importance of cooperation during the attack. If trust develops, most such attacks can be dealt bilaterally or unilaterally.

(c) **Deterrence.** The UN charter and existing international legal framework need to be respected. Policy level framework must be evolved to define the threshold and nature of deterrence. Technological innovations need to be adopted to counter non-attributability so that wrong inferences are not drawn. Also one of the unique characteristics of this domain is that its weapons are not solely controlled by the military / political leadership and also most such weapons are mere softwares residing in obscure covers.

(d) **Legal Framework.** There are three overlapping legal regimes : law enforcement, intelligence collection and military operations that may apply to cyberspace. These activities need to be in synchronisation with international treaties and domestic laws of both originating and intermediate nations. A minimum acceptable legal framework must be defined, so that the same can be ratified in each country, which will enable provisions of legal action based on cooperation among law enforcement agencies.

(e) **Enhancement of Existing Treaties / Conventions.** Most of the conventions/treaties pre-ICT era do not cater to situations arising out of cyber incident/attacks. The framework must identify such provisions and propose amendments. Recent initiative by East West Institute in examining the Geneva and Hague conventions along with its efforts to form a Working Group with Russia and US experts to define various terminologies have drawn attention. More recently, Russia & China have co-sponsored a resolution in UN General Assembly for defining international norms. The orchestration of international accords should be such that norms evolved would limit disruptive activity by some states against other states and deter non-state actors.

(f) **Building Trust.** Embedded hardware systems pose a great threat and provide enormous potential in cyber warfare. Capability for certification of national interests rests in the hands of very few countries. It is necessary to build trust relationship between the nations, so that information technology development can be embraced smoothly and with complete trust. Common criteria group needs to be expanded with equal participation.

Conclusion

Cyberspace has emerged as a major new environment for political and military competition and would necessitate political and military intervention to protect economic and informational interest vital for national security. The challenges for military in the era of on-line connectivity and information flow are unique and require a great amount of coordination among the nations. The challenges get enhanced as cyberspace does not strictly confine itself in military domain and encompasses civilian activities to a great extent. However, governments of many countries are reacting typically to these challenges by expanding their cyber warfare capabilities, yet the politico-military vision that would undermine these efforts are mostly vague and riddled with definitional inconsistency. A joint civilian defence cooperation including public-private partnership and consensus amongst all nations is required to defend the cyberspace in the interests of national security and international stability. Cyberspace should be guided and constrained by political norms and ethical values. Neither the military nor the technological perspective can substitute the strategy for building-up trust and stability for safeguarding international peace and harmony.

*Text of the paper presented at the 7th Northeast Asian Security Policy Forum Meeting held under the auspices of Research Institute of National Security Affairs, National Defence University of South Korea, Seoul on 18 Oct 2011. Theme of the Conference was “Changes in International Strategic Environment and Multi-lateral Security Cooperation”. Brigadier Abhimanyu Ghosh (Retd) was nominated to represent USI at this Conference.

****Brigadier Abhimanyu Ghosh (Retd)** is a Fellow of Indian Institute of Electronics and Telecommunications. Presently, he is the Adviser on Cyber Security with the National Security Council Secretariat.

Journal of the United Service Institution of India, Vol. CXLI, No. 586, October-December 2011.