Cyber Warfare-Dangerous Trends

Lieutenant General Harbhajan Singh, PVSM (Retd)*

Introduction

International and political turbulences have at times led to hacking/defacing of websites across the world. Israeli and Palestinian hackers have launched attacks on websites of each other and India and Pakistan hackers have done the same. There are media reports that in Nov-Dec 2010, intelligence agencies of India and Pakistan (Technical Intelligence Agency and ISI, respectively) fought a proxy cyber war affecting a few hundred government websites on both sides.1 The Chinese have been suspect for a number of cyber attacks in the USA, India and some other countries. These attacks, however, have been rather limited in scope and for short periods i.e. interruptive.

Some Important Cyber Attacks

The cyber attacks on Estonia in May 2007, targeting Estonian Government and private web sites were much larger in scale and lasted nearly a month. They were launched to protest against the dismantling of a Soviet era monument to Red Army in Estonia. But the role of Kremlin has not been overtly confirmed, even though greatly suspected. Quite a few of these attacks were 'Distributed Denial of Service attack'. The attackers used a giant network of 'bots' - perhaps as many as one million computers, located in a number of countries including the United States and pelted Estonian websites/computer systems with hundreds of thousand messages. The attackers even rented some servers to magnify the effect.

It needs to be highlighted that the Estonian authorities were expecting a cyber attack and had erected firewalls around government websites, set up extra computer servers and put staff on call for any eventualities. One of the counter measures taken to block hostile data, was to close off large parts of its network to users outside the country. But still the cyber invaders succeeded.

There was also an incident in 2008 in Iraq. A self-propagating malicious worm was injected into the computer system of the US military, through simple infected items like diskettes and pen drives, which took 14 months to eradicate.

Stuxnet Worm Attack on Iranian Nuclear Plants/Establishments

In September 2010, Stuxnet worm attack on Iranian nuclear plants/establishments hit the international news headlines. This worm also intruded in to industries in some other countries. Stuxnet is a dangerous computer worm which targets Windows Personal Computers (PCs) that oversee industrial-control systems; SCADA. It appears that one of the ways to initially inject could be through use of infected diskettes and pen drives. It then spreads the infection to other computers inside networks that are not directly connected to the Internet i.e. are isolated and thus considered safe. Stuxnet hit some Iranian nuclear facilities, targeting banks of uranium enriching centrifuges and associated controllers made by Siemens. It varied the speed of rotation of the centrifuges to the extent which is reported to have damaged them, retarding the progress on enrichment of uranium for the Iranian Nuclear bomb. 3 The Iranians called it a "nation state Cyber attack" blaming the USA and Israel.

Doctoring the Chips and Kill Switches

'Kill Switches' and 'Backdoors' secretly installed in chips can disable, betray and even blow up the equipment in which such chips are used. 'Backdoors' provide access to the equipment for malicious actions. Chips, microprocessors and printed circuit boards (PCBs) on which these are embedded contain millions of components and circuits. There is, therefore, ample scope to slip in secret codes.

It is possible to make chips which after specified usage become ineffective or on external/programmed command carry out malicious actions. Devices in equipment can be remotely switched on and off whether connected or not to internet. Even a soldier on a PCB can act as an antenna, making possible intrusions from mobile phones/drones/satellites and aircraft. As an example, during Desert Storm in 1991 the Iraqi Forces were using color photocopiers at various headquarters/command posts. The circuitry of some of them contained concealed transmitter which revealed their exact position to American Electronic Warfare planes. This helped in precise attacks on such installations. While most computer security efforts have until now been focused on software, tampering with hardware circuitry may ultimately be an equally dangerous threat. 4

Some years ago Americans discovered Trojan Backdoors in many of the electronics that the US Department of Defence was purchasing from Asian manufacturers, put in at the behest of the Chinese. Strange thing is that the Americans themselves have been using such tricks in equipments supplied by them to their allies and enemies, including by third countries like Canada.

Most Indian civil communications and other networks/applications including critical ones like power sector are importing electronic equipment and components for indigenous manufacture even from countries which are considered to be potential adversaries e.g. China. The possibilities of such equipment/ chips/PCBs having "Kill Switches" and "Backdoors" as also other malware are immense indeed. The Government needs to shed economic and diplomatic considerations where national security is likely to be threatened and ban imports from such sources for critical communication and other infrastructure, as also defence networks / computer systems. Even items like diskettes and flash drives though looking innocuous have been a major source of cyber threat. Cyber security threats are also rising sharply due to proliferation of Internet-enabled mobile devices like smart phones and tablets. These provide new opportunities for cyber criminals to intrude.

Weaponised Cyber Attacks

Considering the above, the world is now looking at a new era of 'weaponised cyber attacks'. This is likely to multiply the power of cyber attacks to much higher and dangerous levels. The head of the US Cyber Command, has recently stated that it is only a matter of time before America is attacked (read other countries), by something like the Stuxnet worm.6 Cyber attacks will not only be able to shut down power grids, air traffic control, banking systems, nuclear facilities and other critical infrastructure but cause damage to electronics and other hardware and corrupt the software controlling them. Such attacks will therefore become more lethal and destructive and corruptive of data and programmes. The scale will vary depending on the resources with the attacker. Most of the preparatory work is being done by such countries on 24x7 basis.

Chinese are supposed to have the largest reservoir of 'cyber warriors'. China's White Paper for 2010 states that the PLA has made great progress in its modernisation and informationisation objectives. As in previous years, the building of new combat capacity to win local wars in conditions of informationisation is emphasised.

Cyber Deterrent

As there is a nuclear deterrent, similarly there could be a cyber/electronic deterrent too, because electronics are all pervasive and nothing works without electronics. No doubt nuclear attacks mean tremendous physical casualties and damage but electronic attacks will immobilise functioning of a country i.e. cause paralysis of the nation and seriously damage its electronic infrastructure. Any deterrent has to be plausible and demonstrated. Spurts of cyber attacks between nations having inimical relations are efforts towards this end and also to test their techniques and responses from other side. Efforts are being initiated to reach international consensus and may be agreements on some rules on use of cyber weapons. The biggest problem is that it is very difficult to locate the source of cyber attacks.

Response to Cyber Threat is based on Past Experience

Generally speaking, in India and other countries measures being taken for defence against cyber attacks are based on the past experience, though new cyber threats are looming. Even for this, resources being allocated in India seem most insufficient. In addition, too many agencies like Ministries of Communications and IT, CBI, NIC and NTRO are involved. There is a dire need for single nodal agency to deal with this critical threat. Our policies, organisations and resources allocated should take into account the futuristic cyber threats and the magnitude of damage and disruption that these could cause. A bureaucratic and incremental approach will invite disaster. Instead, a bold initiative is necessary with the military, central and state governments, industry, academia and more so every citizen participating.

Some Important Measures to face Cyber Threats

Cyber threats have entered the era of nation state cyber and destructive attacks. Also our potential adversaries, China in particular, have made Cyber warfare a key area for waging war. It is, therefore, essential that the criticality of emerging cyber threats is realised at the highest levels of the Government and the Defence Services. This makes it clear that Cyber warfare has to be planned and controlled at strategic level. What is most essential is that a central authority under the PMO, which cuts across bureaucratic boundaries and different ministries and organisations be established, like the Space and Atomic Agencies.

Some of the other measures that are required are as under:-

(a) The government and industrial as also military infrastructure should be made ready to absorb new destructive attacks and recover quickly.

(b) There is a need to practise 'Active Defence' as compared to 'Passive Defence'. Active Defence entails "before event efforts rather than after event postmortems".

(c) Locate bugs/malware that may have already penetrated systems and could be lying doggo. Sources of and how these penetrated the system must be identified and loop holes plugged.

(d) A national effort to identify infected computers and clean them up needs to be undertaken. All users should be encouraged to report every malicious cyber incident. South Korea and Germany have tackled this problem by setting up national call centres to which Internet Service Providers (ISPs) can refer infected customers to get advice about disinfecting their computers.

(e) One of the essential remedy lies in manufacturing latest chips for critical equipment in safe foundries. Making chips is a strategic requirement, for which commercial viability should not be a criteria. In addition, even though difficult, maximum possible testing should be undertaken, which requires creation of needed infrastructure.

Need for a Cyber Command. For the Defence Services a Cyber Command is a must, which will coordinate the cyber activities of the three Services. Success in Cyber warfare cannot be assured if we work in penny packets and uncoordinated manner. Unity of command is a pre-requisite. The Cyber Command could be a tri-service command on the lines of the Strategic Forces Command and functioning under the Chiefs of Staff Committee / CDS (as and when created). It will have three Services components suitably structured as well as a Joint Operations Centre which will control both defensive and offensive operations. The Command should have lateral linkages with the National Cyber Authority and the National Security Adviser, and ought to function in close coordination with them during peace and war.

Security of Defence Networks

As for Defence Networks, critical ones must be isolated and a "secure zone" created. Isolation requires totally separate media ensuring end to end quarantine and also isolated access devices like laptops/tablets and PCs. Quite a few of the Defence Networks in the rear areas are engineered on civil media/networks. These can become highly vulnerable to penetration and attacks and act as Backdoors to so called isolated Defence Networks. Also, electronic and physical

security measures, particularly at nodes assume critical importance.

The threat posed by malware concealed in chips/PCBs and equipment from foreign/unprotected local sources has assumed very dangerous proportions. This needs to be plugged on emergency basis. The Defence Services have to lay down security rules and regulations in this regard for equipment and networks they are going to use, whether own or hired, and ensure that indigenously manufactured, fully tested components are used and no diplomatic/economic/political considerations are allowed to dilute or bypass these.

Declaring a Cyber Attack an Act of War

The USA is seriously thinking of declaring cyber attack as an act of war, depending on its severity, as it can cause destruction/disruption comparable to a hostile conventional attack and would take retaliatory actions - weaponised or others. This is a very significant development and shows how seriously the US takes cyber warfare.

Concluding Remarks

Cyber warfare cannot win wars on its own, but its indirect approach could succeed where direct action cannot. Cyber warfare operations must be synchronised with those of other war fighting domains and can act as force multiplier. Cyber threats have assumed dangerous proportions and cyber attacks have become destructive and not just interruptive. Our potential adversaries; China in particular, are laying great emphasis on Cyber warfare and developed considerable expertise and infrastructure. India needs to realise the dangers posed and make this a key area.

There is a need for a centralised organisation under the PMO to coordinate the efforts of different agencies involved. The Defence Forces should have a Cyber Command coordinating the efforts of the three Services. Fragmented efforts in penny packets will not suffice. Individuals who are mission oriented should be put in charge as Cyber warfare is 24X7 happening even during peace time!! Young computer experts should be offered lucrative remuneration to attract them to specialise in Cyber warfare as against having a career in normal software work.

Imported electronic components and equipment including chips and even innocuous CDs and Pen Drives are doorways for deadly infections and damage to the systems they are used in. Even so called friendly countries cannot be trusted. India needs to be self sufficient in manufacturing such hardware and in particularly latest chips/microprocessors, to prevent cyber attacks.

Last but not the least, no nation can come out victorious in any warfare including Cyber warfare, unless it takes offensive action. India should develop credible offensive capabilities in Cyber warfare and let it be known to the world, so that other nations are deterred from messing with India’s electronic systems. India has the brains and software competence which are at par, if not better than any other country. What is needed is political will and setting up proper organisations bereft of bureaucratic interference and inter-agency rivalries/turf wars.

*** Lieutenant General Harbhajan Singh, PVSM (Retd),** of the First Course National Defence Academy and 10th Regular Course IMA, was commissioned into the Corps of Signals in Dec 1952. He retired as Signal Officer-in-Chief in Jan 1991. Post retirement, he has been writing on National Security and Military matters.

Journal of the United Service Institution of India, Vol. CXLI, No. 584, April-June 2011.