Cyber Security and Intelligence

Challenges and Way Ahead

CLAWS RESEARCH TEAM

India faced the largest strategically targeted cyber attack on 12 July 2011 when a large number of computers in the offices of the PMO/MHA/MoD/MEA handling sensitive security related information were targeted. A mass of emails from one address with an attached word document titled 'cms,ntro:dailyelec.mediareport (2011)' were sent to inboxes of key officials of India's vast security architecture. These were well-planned attacks meant to launch selective commands on the system that would be saved on a virtual drive created secretly by the malware. Mass attacks on India's key security-related ministries were also reported in the months of April and May this year. Some reports also suggest that the fault in the power sub-station which resulted in a blackout at New Delhi's T3 terminal on 08 Aug 11 was a planned cyber attack, though no evidence has been given to support the proposition. Elsewhere in the world, in April this year, Iran accused Israel and the US of launching a computer worm designed to sabotage its nuclear facilities. Such incidents are occurring with increasing frequency across the globe.

The above incidents have been highlighted to illustrate the grave danger which we face today through cyber attacks. These attacks symbolise a form of warfare which will increasingly be used and for which we need to guard against. These can take the form of espionage, sabotage, disruption of data bases, communication systems, financial systems and the like. In fact, any system which uses computerised systems for functioning is under threat. Military activities

that use computers and satellites for coordination are at risk of equipment disruption. Orders and communications can be intercepted or replaced. Power, water, fuel, communications, and transportation infrastructure all may be vulnerable to disruption. The equipment procured through foreign vendors can be manipulated to launch cyber attacks in a clandestine manner. The possibility of the entire economy of a country coming to a grinding halt through cyber attacks is now a very real threat. It is therefore imperative that we upgrade our cyber security to meet the challenges of cyber attack.

There are four pillars to the cyber war realm: intelligence, technology, logistics, and command. Information is power in today's world. Also, to be forewarned is to be forearmed. Intelligence hence would remain the key component in countering the threat of cyber attacks.

Cyber Intelligence constitutes new data and information gathering resources, technologies, capabilities and techniques. Many of the current intelligence gathering platforms offer little or no cyber threat intelligence gathering capabilities. This is because unlike nuclear weapons and other weapons of mass destruction, cyber weapons and attacks require far less infrastructure and do not require restricted materials or knowledge that is in limited supply. It is extremely difficult to cloak the return path for information obtained from the cyber bugs that compromised computer systems.

Cyber Warfare Intelligence addresses the process of gathering data and information about a cyber enemy or threat. This represents the data collection, analysis and interpretations that lead to insight and understanding that is specific to the cyber threat operational environment. The defence forces for obvious reasons are one of the prime targets of cyber warfare. The collection of cyber threat intelligence presents the most significant challenge for the defence intelligence community. Developing cyber intelligence requires digital trespassing on foreign networks and the computers operated by foreign governments, corporations and individuals which is a time consuming and risky affair. This underlines the importance of availability of suitably trained operatives for cyber intelligence.

Most cyber attacks leave behind forensic evidence that can be used to assess the capabilities of the attacker which could give an insight into the entities behind the attack. Significant evidence pertaining to techniques, cyber weapons, and strategies used in these cyber assaults can thus be obtained which should be exercised, processed and turned into intelligence.

One of the unique aspects of cyber weapons is their ability to be launched from anywhere. Computers that are physically located in other countries can be

compromised and used as a cyber attack launch platform. We need to develop forensic investigative capabilities that can trace these attacks to the origination point, but establish the parties behind the attack.

Cyber counter-intelligence are measures to identify, penetrate, or neutralise foreign operations that use cyber means as the primary tradecraft methodology, as well as foreign intelligence service collection efforts that use traditional methods to gauge cyber capabilities and intentions.

The Challenges

The challenges of cyber intelligence will require rethinking of our intelligence infrastructure as well as the development of new intelligence assets and technologies. In addition, the extremely limited infrastructure available to develop and deploy cyber weapons, ascertaining if the attack was from a terrorist or extremist organisation or nation state versus an individual acting on its own is likely to challenge the intelligence community in times to come . The collection of cyber threat intelligence presents the most significant challenge for the defence intelligence community as well as the commercial industry.

Shortage of Trained Manpower. The government and private sector computer networks would not be able to prevent attacks from foreign countries, criminal organisations, terrorists, and hackers, unless there is a significant increase in the number of cyber security experts. It has been repeatedly demonstrated that the challenges of cyber security and cyber intelligence far surpass the number of skilled professionals and technical solutions available to attend to these issues. Thus, it is necessary and urgent that new generation of specialists in cyberspace security is properly educated. Challenges in the public and private sectors are many and not nearly enough sufficiently prepared young people are to be found to face these challenges.

Lack of Adequate Computer Literacy. This requires that new leaders be trained in computer sciences through programs that perfect their aptitudes and teach them how to properly apply the knowledge they acquire to vigilance, detection, analysis, and faster responses to possible infiltrations in their networks.

Insufficient Research and Development Instinct. Another important challenge is to foster badly needed research and development instinct and encourage innovative thinking. The development of infrastructure and equipment for cyber intelligence needs 'out of the box' thinking to match their counterparts who have access to better infrastructure.

Way Ahead

Public-Private Partnership.

In terms of information security, many of the intelligence community's cyber threat issues are similar to those faced by the commercial sector as well. Commercial industry far outstrips intelligence community information technology investments. The field of cyber intelligence presents great and interesting opportunities for collaborations between the public and private sectors.

Presently the cooperation between businesses and government has a wide scope of improvement. 'Defence' is one of the departments most affected by cyber attacks and is also one of the departments that can benefit the most from this collaboration with the private sector. Another area where vital public-private action is required is in the promotion of computer sciences education throughout primary, secondary and university level schooling. Computer science education and training must be given priority not only in public service campaigns, but must also be promoted by private enterprise.

The Office of the US Director of National Intelligence's (ODNI's) cyber goal is "data finds data at net speed," However, the intelligence community does not know how to achieve that goal yet. US has embarked on a path to achieve this goal through collaboration with commercial industry. It is recommended that we in India especially defence forces should also exploit this expertise.

Cyber Counter Intelligence (CCI)

CCI covers the measures to identify, penetrate, or neutralize adversarial operations that use cyber means as the primary tradecraft methodology. CCI activities in cyberspace include those forensics examinations of information systems and other approved virtual or on-line activities to identify, disrupt, neutralise, penetrate, or exploit hostile adversaries.

Conclusive Analysis

Threats to cyberspace pose one of the most serious economic and security challenges of the 21st Century. However, it is pertinent to note that cyberspace also offers us unprecedented opportunities to shape and control the battle space to achieve strategic objectives .Cyber capabilities are a critical aspect of modern day warfare and as such must be integrated into military doctrine. A number of nations are incorporating cyber warfare as a new part of their military doctrine.

The challenges of cyber intelligence will require rethinking of our intelligence infrastructure as well as the development of new intelligence assets and technologies. Challenges in the public and private sectors are common to both as they are equally affected by cyber attacks. The educated human resources to collect cyber intelligence are in short supply and needs immediate corrective measures. To this end, computer literacy has to be further enhanced. More is needed, however, in terms of understanding what's at stake in cyber security, improving intelligence regarding adversaries' capabilities, intentions and activities, and creating the mechanisms to couple the public sector's capabilities to the private sector's needs. The government should consider how best to improve our cyber intelligence, so that our capabilities of cyber intelligence can contribute to a global cyber strategy that defends our national and economic security interests.