Dhiraj Kukreja*

Securing Cyberspace

Abstract

Cyber-security is thus a very serious issue. Attacks can have catastrophic consequences. The cyber-war is for real. Greater legal certainty, less confrontation between departments and more cooperation between governments, is the call of the hour. India has to make cyber-security a priority, if the government wants to go digital. Attitudes and behaviour have to change.

Introduction

Almost 33 years ago, William Gibson, an American-Canadian author of the popular sci-fi novel, *Neuromancer*, coined the term "cyberspace" and envisaged a future, in which hacking would be a norm, and giant corporations would be actually raiding each other's computer systems in search of secrets. He was more or less right in his predictions about these future trends that he foresaw almost 3 decades ago, in 1984. He was slightly wrong about some of the pertinent details though; i.e. today, the governments of warring/ competing countries, not corporations or anti-social teenagers, have become the world's best hackers.

Though hacking has apparently become a constant threat and a major irritant, much more cyberspace activity substantially crosses the screens of watch-centre monitors, backstage, hidden from sight and unknown to the public. The Chinese, the Russians, the Americans, the Israelis as well as many other known and unknown players, use hacking in one way or another, for a spectrum of reasons ranging from espionage, extortion, damaging enemy systems, or simply as an irritant.

* **The author** is former Air Officer Commanding in Chief of Training Command, Indian Air Force.

A very recent example of just such an hacking event was detected on 23 November 2016, when Symantec, an American antivirus firm, announced the discovery of a piece of software called 'Regin' (the arbitrarily chosen name comes from a text string found in the bug's innards), which it had found lurking on computers in Russia, Saudi Arabia and several other countries, sniffing for secrets. Its sophistication and stealth led Symantec to conclude that it must have been written by a nation-state. Another recent malware attack, which surfaced on the 12 May 2017, caught the world's attention was called the ransomware 'WannaCry'. It broke new ground and showed how digitally vulnerable we actually are.

History of Malware / Ransomware

Working out who has created a piece of malware is not easy. Unfortunately, computer code has no identity or nationality. Programmers sometimes leave hints, or use suggestive phrases, but these cannot be considered as actual proof that they were the creators. The targets, on the other hand, can provide substantial clues as to the origin, as can comparisons with known, existing malware. 'Regin', so far, is only the latest in a long line of known government-sponsored malware (see table).

What did you expect, an exploding pen?
Selected government malware

Year discovered	Malware	Possible source
2006	Greek Vodafone hack	?
2010	Stuxnet	US and Israel
2010	Aurora	China
2012	Flame	US and Israel
2013	Red October	Russia or China
2014	DarkHotel	South Korea
2014	Uroburos	Russia
2014	The Mask	?
2014	Regin	Britain and US

Source: The Economist, 27 November 2014.

The most infamous of malwares, in the above list, is 'Stuxnet', discovered in 2010, which was designed, almost certainly by America and Israel, to hijack industrial-control systems. It was deployed against Iran's nuclear installations, and destroyed centrifuges that were being used to enrich uranium. This sort of direct sabotage carried out by Stuxnet was most unusual, as most government

malware that security researchers know about, are generally designed for gathering information rather than sabotaging systems. In 2006, for instance, it emerged that someone had hacked electronic equipment belonging to Vodafone's Greek subsidiary and eavesdropped on the mobile-phone conversations of the Greek cabinet. Such information-gathering attacks, can however, also inflict damage; China has a long history of pilfering military secrets from foreign computers (vigorously denied by them as can be expected). Unlike the vast surveillance dragnets revealed by Edward Snowden, a former American contractor who leaked thousands of secret documents in 2013, these computerised bugs are tailored and aimed at defined targets, to gather information.

WannaCry, one of the latest but definitely not the last, in a long list of malware, surfaced on 12 May 2017, exploiting weaknesses in older versions of Windows, especially Windows XP. It locked down computers and servers, demanding a hefty ransom for unlocking them. The National Security Agency (NSA) of USA was the first to notice this weakness of the Windows operating systems, but did not share this valuable information with the world. Instead, it developed tools to exploit this weakness, where and when required. Unfortunately for them, these tools in turn were hacked and taken over by a group, in mid-2016. The creators of WannaCry used these very tools to infiltrate the systems in about 150 countries. The ransom demanded payments in bitcoins, (cryptocurrency) equivalent to about 300-600 USD. A North Korea based group, the Lazarus Group, is suspected for initiating this latest attack; this group is also reportedly associated with earlier attacks on the South Korean Government in 2009-12, the Sony Pictures in 2014, and the heist on the Bangladesh Bank earlier this year, when about $ 81 million was siphoned off from the bank. In this latest attack, it is suspected that the group was also holding to ransom the Disney Pictures for a yet unreleased movie.

Ransomware is not a new phenomenon. The first recorded attack was in 1989, distributed on floppy disks, via post. The floppy disks were supposedly distributed to measure an individual's risk of susceptibility to AIDS, but instead had an embedded virus that encrypted all data once the PC was restarted 90 times. Another ransomware, the CryptoLocker was probably the most prominent and the most damaging, and had affected more than 250,000 computers between September 2013 and November 2013. The perpetrators made millions before the virus was destroyed in 2014, in a concerted worldwide effort. After the CryptoLocker was taken down, clones appeared and became active between 2014 and 2016 as CryptoWall and TorrentWall. By mid-2015, CryptoWall had

extorted in an excess of $ 18 million! There are other ransomwares, TeslaCrypt or Alpha Crypt, Locky, Petya, and Jigsaw, which, as per reports, continue to be active in some form or the other, extorting money in bitcoins, through PayPal or direct payments in bank accounts.

Cyber-Security: Is it a Myth?

Computer security is a contradiction of terms, in itself. As mentioned above, in the past year alone, , cyber-thieves have managed to steal $81 million from the Bangladesh Bank; almost derail a major economic transaction between two IT giants, Yahoo and Verizon,; and now allegations are flying high about Russian hackers having interfered in the last US presidential elections. Besides, though not so well known, there looms the threat of black markets, where computerised extortion, hacking-for hire and disposal of stolen digital goods, are the norm. The problems can only get from bad to worse!

Another major issue is the detection of the author of a piece of malware, which is not at all as easy as it appears. This difficulty makes cyber-espionage and cyber-heists so very attractive. The other problem is that modern software is so complex, that it is riddled with major security lapses, most of which can be unfortunately, exploited from a safe distance. Once a hole is found in the fabric of the software, the data can easily and cheaply be smuggled out and sent around the world, in a matter of seconds!

Increasingly, nowadays, computers are not just dealing with abstract data like credit card details, but also with real world objects like automobiles, aircrafts and even the vulnerable human body. Hackers have already displayed their skills by their ability to remotely take over cars that are connected with the internet, and even pacemakers installed in the human body! It is tempting to believe that further advancement of technology resulting from this call for heightened security awareness, may solve some of the the security problems, but there appears to be no fool-proof way to make computers completely safe.

Computers generally run on software that is immensely complicated and intricate. Across all its products, Google manages about two billion lines of source code; so much of information that errors seem inevitable, therein. An average programme has 14 separate vulnerabilities, each of which is a potential point of illegal entry, waiting to be exploited. It is almost next to impossible to shut down every illicit entry point. “The attackers have to find one weakness,” says Kathleen Fisher, a computer scientist at Tufts University in Massachusetts, “while the defenders have to plug every single hole, including the ones they do not know about.”

The problems lie just not with hacking into software, but even in the manufacture of computers. All modern computers work on chips, which are typically designed by one company, manufactured by another, and mounted by yet another, who mounts it alongside other chips, which may also have been procured from other firms. Peter Singer, a fellow at New America, a think-tank, mentions of a fault detected in 2011, in some of the transistors of a chip, on-board US Navy helicopters. If the bug had not been detected, the helicopters would not have been able to fire its missiles. Investigations revealed that the chip had been manufactured in China, but could not point a definitely accusing finger on whether the fault was accidental or intentional!

Most hackers do not have the resources required to fiddle around with chip designs and manufacture, hence hacking is either an undemanding show of mischief or a criminal act, which is actually also easier. Stolen credit card details are sold in the 'black market' in cyber space in batches of thousands at a time; data dealers sell information on weaknesses detected in software; ransomware is available not just for purchase, but also can be rented by the hour. The market is so sophisticated that coding skills are optional. The total cost of hacking is anybody's guess, but it is only going to get worse, because the scope is increasing with the development of "Internet of Things" (IoT), which will computerise everything from cars to power meters to toys to homes and medical devices. The increasing computer and cyberspace insecurity, however, has triggered companies, academics and governments into action.

In cyberspace, it is not just hacking that the world has to deal with. The scourge of modern times, terrorism, is also utilising cyberspace to its advantage. As long as there have been data networks, people have exploited them to their advantage. The French mechanical telegraph system was corrupted in 1834 in a bond-trading fraud, which went undetected for two years! The internet today, is the most powerful network of all, with billions of users and unlimited processing capacity; it should be of no surprise to anyone that it has come in the focus of wrongdoers.

The internet is enabling terrorists and promoting their activities at an exponential rate; a speed that has caught the security agencies off-guard. The use of cyberspace has become even more refined since 2014, when the IS established its caliphate in parts of Syria and Iraq. The ubiquity of internet has been used by the IS to hawk its propaganda online to recruit followers, promote its ideology, proclaim its social and military achievements, and spread fake news about the non-believers, the *kafirs*. Similar is the case with other groups, be they in the Middle East, South East Asia, India, or Afghanistan.

Enhancing Cyber Security

The biggest challenge facing the governments and the corporate world, which are the main bodies under attack by hackers for whatever reasons, is the availability of qualified cyber warriors, in sufficient numbers. Even as this piece is being written, there is news of another massive attack on computer systems in many countries around the world, akin to the earlier WannaCry ransomware, indicating that the kill-switch for the previous attack was not nearly as effective as previously thought. Hostile computer activity from spies, saboteurs, competitors, and criminals has given rise to an army of defenders, more in the corporations and comparatively lesser in the government cyber units. The demand for specialists, however, has far outpaced the number who can do the job, leading to a staff crunch, especially in the government units, which are more susceptible to poaching.

So how does one get the cyberspace more secure? Most cyber expertise remains in the private sector, where companies are seeing a substantial part of their budget diverted towards security products and services. Depending upon the nature of the threat, private companies are bidding for cyber talent, but recruitment and retention continue to remain a challenge. A graduate with a good computer studies degree can walk into a high six-figure salary, with an equivalent amount as a golden handshake, which would be several times higher than what a government agency would be likely to offer.

It would be prudent to accept that one's computer systems are vulnerable to an attack, and will be attacked, more sooner than later; the strategy against such an attack could be either passive or active. The former method is essentially target hardening, which largely consists of the use of various technologies and products, for example, firewalls, cryptography, intrusion detection, and standard safety procedures, such as those governing outside dial-in or reconstitution and recovery, with an aim to protect the assets. By definition, passive defence does not impose serious risk or penalty on the attacker. On the other hand, active defence, by definition, imposes serious risk or penalty on the attacker. Risk or penalty may include identification and exposure, investigation and prosecution, or pre-emptive or counter attacks. This is a task, easier said than done, since most attackers remain behind a shroud of anonymity.

A basic approach is to design the system to be secure from an attack, right from its conception. Unfortunately, for a vast majority of IT systems, security has not been a major design criterion, if it was considered at all; even the original Advanced Research Projects Agency Network (ARPARNET), developed by the US Department of Defence, was considered susceptible to attacks due to

design flaws. If security were made a major design criterion for a new system, there is little doubt that it could be made more secure than most of its predecessors. However, there should be no delusion that newly designed large, complex systems can be kept safe and secure in today's world!

Since security was not a part of the original design in almost all cyber-systems that are in extensive use, the world today has an enormous legacy of insecure systems. Improving security for such systems, therefore, is largely a matter of afterthought and patchwork. The problem is compounded by the fact that security patches are often in conflict with the initial design; a modification in design for added security is, therefore, not just costly, but may also result in reduced efficiency and functionality.

For the governments and corporations that are repeated victims of cyber attacks, the biggest challenge is finding cyber warriors with the right qualifications and in sufficient numbers to ward off these attacks, and also fight back. Many countries and organisations, both civil and military, have established cyber forces to fight back, but it is a task not so easy, for the demand for experts has thus far outpaced the supply.

India Prepares for Cyber War

Cyber security, a relatively nascent project in India, has not kept pace with the growth of the IT sector; cyber crime was categorised as a punishable offence only as late as 2008, when the government promulgated the IT Act 2008. This came at a time when official data was now increasingly being stored online and hostile neighbours and extremist groups were garnering their resources and expertise for an all-out cyber war; not only China and Pakistan, but even USA was nosing around for official information. The most frequent incursions were noticed in the PM's office, Ministry of External Affairs (MEA) and Ministry of Defence (MoD).

As is with all countries, India too, began readying itself for defence against a cyber attack, and as is with all countries, not much is known in the public domain, barring a few, scattered news items ("India Readies Cyber Army to Spy on Hostile Nations, *Times of India*, 05 August 2010). After a spate of attacks starting from 2007 (see table) on its computer systems, a strategy of taking the fight back to the hackers was formulated in a security meet, chaired by the then National Security Adviser (NSA), Shiv Shankar Menon, in early August 2010. Some of the salient outcomes of the meeting were:

(i) A pilot Joint Working Group (JWG) under the NSA, proposed the creation of a permanent JWG, under the National Security Council

Secretariat (NSCS), which falls under the National Security Council, headed by the PM.

(ii) The JWG would be an advisory body and will coordinate public-private partnerships.

(iii) The setting up of a Joint Committee on International Cooperation and Advocacy.

(iv) The private companies would set up their cyber security infrastructure and share their knowledge with the NSCS and others in the sector, to protect Indian companies from cyber attacks.

(v) The creation of testing and certification centres and pilot projects for conducting test audit on IT products.

	Phishing	***Probing***	***Virus/Malware***	***Spam***	***Website Attacks***	***Others***
2004	03	11	05	-	-	04
2005	101	40	95	-	-	18
2006	339	177	19	-	-	17
2007	392	223	358	-	-	264
2008	604	265	408	305	835	148
2009	374	303	596	285	6548	160
2010	508	277	2817	181	6344	188
2011	674	1748	2765	2480	4394	1240

Source: CERT, *ET Magazine*, 13-19 October 2013.

IT workers and ethical hackers who would have been recruited for the ambitious project are supposedly protected by law; as per Indian law, hackers are punishable with imprisonment of up to three years, or a fine of up to Rs two lakhs, or both. Their expertise was planned to be used, not just for defence, but also to go on the offensive or carry out pre-emptive strikes against hostile countries.

As per available information, the government's cyber security plan, formulated in mid-2013, looked at getting together institutions like the National Technical Research Organisation (NTRO), MoD, MHA, CERT-In, and other related agencies to work towards a common cause, with NTRO as the umbrella organisation, working in close liaison with the Defence Intelligence Agency (DIA). The move was welcomed in legal and IT organisations, as a belated measure against a growing menace; however, turf wars between the many official agencies hurt a coordinated approach in cyber security. In the meanwhile, the private sector has forged ahead with their plans of creating PPPs, developing security solutions and sharing or selling the solutions.

In sheer numbers, recruitment should not have been a major problem. As per Nasscom, the country produces more than six lakh professionals, who are technical graduates or post-graduates; this massive number is complemented by the teeming workforce in R&D, anti-virus, and software centres of Indian and international companies. To ensure a steady 'supply' of IT professionals, the NSA Secretariat also directed the HRD and IT ministries to introduce cyber-security as a subject in the curriculum of IITs and other educational institutes. Notwithstanding the efforts, the known figures state that India has only around 600 professionals working with the government, compared with about 125,000 in China, 100,000 in USA and 75000 in Russia.

Despite the NSA's measures to enhance cyber-security, attacks continue to take place at regular intervals and with varying intensity, and the available remedial measures have not actually been very effective. In late 2010, the website of Central Bureau of Investigation (CBI) was hacked and was back in business after a fairly long break of more than three days. On Republic Day in 2014, Pakistani hackers defaced a total of 2118 websites, including those of some prominent public sector banks, in what was then termed as a major cyber attack. The Global Cyber Security Response Team (GCSRT), based in Bengaluru, confirms that this 'major attack' came two weeks after 1400 sites were hacked!

Although the government has circulated Computer Security Policy and Guidelines to all the ministries and departments on taking steps to prevent, detect and mitigate cyber attacks, the flurry of attacks continue. Pavan Duggal, a known cyber-lawyer and an expert on cyber-security, told rediff.com in December 2010, "India has not notified most of its sensitive government sites as protected systems, despite the IT Act being in place since 2008. This shows a lack of seriousness in fighting cyber related issues." This lack of seriousness, is due to a lack of understanding of the gravity of the problem.

Along with the small group of hackers or computer experts who help the government, there is a one well-known industrialist who has taken the bull by the horns. Mukesh Ambani, Chairman of the Reliance Industries Limited (RIL), floated a plan to develop security solutions for captive use at its many business sites.

Concluding Thoughts

Cyber-security capabilities are of great importance, as cyber-space will be the fifth dimension of future warfare, the others being air, land sea and space; within these capabilities, offensive capabilities are essential. The power of an offensive attack cannot be overlooked after attacks with cyber-weapons like

the Stuxnet, Flame, WannaCry, Petya and others. Alongside this, the defence capabilities also need to be bolstered. Most government officials do not have the knowledge, and some even lack awareness, of how to handle such threats and are thus vulnerable to attacks such as spear-phishing or probing, which target them to enter the system through spoof emails.

The rules of engagement of cyber warfare are still incomplete and continue to be written everyday. Even the best of armies, are not yet fully prepared for a full-blown cyber attack. One reason why computer security continues to be so weak could be because very few were serious about it yesterday. Now that the consequences of cyber attacks are known, and the risks posed by malware and bugs are large and growing, there is no excuse for repeating the mistakes of yesterday.

So far, India has managed to escape an attack like the Stuxnet, but the possibility always exists. Espionage, mischief, or harassment may be the sole motive of attacks of overseas hackers, including that of our neighbours. An offensive, a distinct possibility could be directed against our infrastructure or even the political system. Imagine a scenario: there can be a total blackout through a power grid failure; this had occurred a few years ago but the actual reasons have not been revealed till date. With an increasing number of cities opting for the metro train services, and the Indian Railways too upgrading its services, the transport and the rail system can be hacked and crippled. The Indian economy is following northbound; what if the stock exchanges and banks are hacked? Elections can be stalled or influenced or the government can be toppled through the spread of fake news, propaganda, as is suspected to have happened in USA. These are just a few examples; the list is endless.