MARITIME AFFAIRS Copyright © National Maritime Foundation
Vol. 8 No. 2 Winter 2012, pp. 73–94
Print ISSN: 0973-3159, Online ISSN: 1946-6609, http://dx.doi.org/10.1080/09733159.2012.742653

Routledge
Taylor & Francis Group

National
Maritime
Foundation

Contours of Security in Cyberspace

Wg Cdr Sanjay Poduval*

The cyberspace is an intangible medium operating and controlling many aspects of the tangible world. It is a world without barriers therefore artificial barriers have to be erected to prevent free ingress or egress. This is a world still in the nascent stages of its evolution; therefore to stay ahead of the pack we need to be imaginative and innovative. The increasing interconnection of the world's computers, standardization of communications protocols and computing hardware enable a single worm developed attack many systems. This provides attractive avenues for cyber attackers to exploit. Complementing these features, are today's cyber criminals who are increasingly adept at gaining undetected access and maintaining a persistent, low-profile, long-term presence in IT environments. Moreover difficulties in identifying attackers, coupled with an uncertain legal and policy framework, make it difficult to punish the offenders. Therefore, one has to take proactive steps, be vigilant and increase the cost of intrusions to keep unwanted visitors at bay. Today cyber attackers, armed with constantly evolving malicious code are likely to have more paths into a network and extract the secrets it contains making the task of the system administrators a herculean one. The elegance of computer hacking lies in the fact that it may be attempted for a fraction of the cost; all one requires is a laptop connected to the internet and a lot of patience. With this in mind the paper attempts to give an insight into the various contours of cyber security which should be a valuable tool in appreciating the vulnerabilities of the cyberspace.

*Wing Commander Sanjay Poduval was a Research Fellow at the National Maritime Foundation, New Delhi. He can be reached at sanjaycaps@gmail.com

Introduction

The promise of cyberspace has touched nearly every aspect of our everyday lives in some form or another; from the television which provides entertainment to the internet that delivers our emails, helps close business deals or reserve our tickets or the cell phones we use to make calls and return text messages. It also helps run businesses, control essential services like water, transportation, electricity and banking which often help save time and trouble; the contours of cyberspace are all around us. These wonderfully convenient inventions are so prevalent that we frequently take them for granted. But there is no coin without its flip side and therefore, the virtual world too has given rise to a population which aims to turn this beneficial development to their advantage whether for financial gain or in pursuit of a social or political agenda, or even for the pure malicious challenge it offers. The cyber world is an intangible world, operating and controlling many aspects of the tangible world. The operations in cyberspace cannot be heard, seen or felt (for example, in the tangible if there is a break-in one could actually see the process taking place but it is not so in cyberspace, a malware may be resident in the system unknown to the host and siphoning data to its master located somewhere in the globe) only the end result is noticeable. Therefore, the constraint in cyberspace is the appreciation of the problem of the many contours of security as there are no visible signs of ingress or egress. This essay will delve into some of the contours of security in cyberspace.

Classification of Cyber Security

Security classification can be carried out in a number of ways, for example, intention of the players, type of players, costs involved, technology and technicalities involved and also on the type or criticality of the target. All these have overlapping and common features. For the purpose of this essay cyber security has been classified into the following four broad categories:

1. acts with mischievous intent;
2. acts with Criminal intent;
3. acts by vested interests; and
4. acts by nation-states.

Mischievous Intent

These are harmless, irritating acts not aimed at disrupting or damaging the targeted systems. These could be in the form of defacing websites which require a very low level of expertise but is largely harmless. These could be in the form of a disgruntled employee sending inconsequential emails to his colleagues to settle scores with them or pranks by tech savvy students randomly penetrating sites in which they find loop holes. These types of attacks of course need to be tackled but are not intended to disrupt or destruct; the aim is to cause minor disturbances. The operations of this nature can be confined to this category as long as information gleaned from these attacks are not escalated to the next three categories. The costs involved are normally on the lower side. There are, however, others who take advantage of these loopholes, create backdoors and remain inside without causing any trouble till the need arises.

Criminal Intent

The attacks in this category are carried out with the intent to disrupt the targeted system. The *modus operandi* of the attacks in the next three categories is largely similar, but the distinguishing factor between the three types is the kind of information exfiltrated. In case of an attack with a criminal intent the data stolen is used to gratify the personal needs of the perpetrator. For example using the information of bank accounts and their passwords for cash transactions, or destruction and disruption of systems for self gratification in response to a self-perceived injustice meted out, or to avail monetary benefits. There are also cyber hackers not interested in stealing money directly, as it could land them into trouble. These groups are more interested in stealing peripheral information such as contact details, identity numbers, etc., that can be sold on the black market at a later date. The global black market for email addresses and national identity numbers is now worth about $5 billion, making it a lucrative area for hackers looking to steal contact information. Attacks of this nature can cause grave damage to systems, targeted firms or to the individual concerned. The following can be classified as criminal acts:

- denial of service attack;
- spreading of m-codes;
- software piracy;
- credit card fraud;

- phishing;
- net extortion;
- cyber stalking;
- cyber defamation;
- threatening; and
- salami attack.

Acts by Vested Interests

Wikileaks and industrial espionage are the best examples in this category. Of course Wikileaks is not the classic cyber-attack, but the cyber infrastructure was definitely used for its propaganda. These attacks have the potential to either cause severe embarrassment to the targeted states or organisations or cause serious monetary loss when design details of sensitive equipment and IPR (Intellectual Property Rights) are pilfered or when classified notes, conversations and documents are revealed to the outside world. There are also ''hacktivists'' who break into networks largely just to disrupt them and make a political point. The cost and sophistication associated with these attacks will depend on the type of organisation perpetrating. For example if an individual is perpetrating the attacks the costs will be on the lower side where as if it is a larger organisation the technicalities and the costs will be much higher.

Acts by Nation-States

The category of data accessed in this case does not have monetary value associated with cyber criminals. The focus is mainly on documents related to technical, defence engineering information, military related information, or government policy and analysis. Documents of this nature are not easily monetised by cyber criminals unless they have a nation-state customer, which makes the activity state sponsored or state encouraged. These acts are also characterised by a high level of obfuscation because of the need to remain in the shadows. The numbers of proxy sites servers are spread around the globe which makes it very difficult to trace the origin of infiltration. The use of zero-days which are a costly proposition are very high.

When a nation-state gets into the act of creating a virus it becomes qualitatively different from what few hackers (or crackers) can do; what was at best a nuisance and at worst a loss of some data from infected machines can transform into a complete breakdown of the basic infrastructure of a country. A nation-state has the ability to target computers that control vital infrastructure and cause catastrophic failures of the system. Even when specific equipment or a country is targeted, as Stuxnet has shown, such worms can escape beyond their targets and pose a threat to other equipment and other countries as well.

All of the above can of course be carried out by insiders, which is by far the most efficient of penetration. The most prominent feature of an insider attack is that the level of success is very high. The insider knows the functioning of the system very well and will directly go for the vulnerable points in the system. The level of brute force on the system is therefore very low. A high degree of sophistication is not essential since the insider can hit the bull's-eye every time. The characteristic feature of this type of compromise is that a log analysis will probably not yield any false positives[1] because no illegitimate operation had been performed.

Modus Operandi

Cyber-attacks exploit vulnerabilities of software, both operating systems and applications. Unfortunately, the increasing standardisation of software means that military organisations often use the same software as civilians do, and much of this software has the same vulnerabilities. Many viruses and worms that could cripple a civilian network could just as easily cripple a command-and-control network. The increasing interconnection of computers through networks means there are many routes by which an attack could spread from ''innocent civilian bystanders'' to those of a military organisation's computers. Military systems try to isolate themselves from civilian systems but are not very successful because access to the internet simplifies many routine tasks. Furthermore, information flow from civilian to military systems is often less restricted than flow in the other direction, which actually encourages an adversary to first attack civilian sites.

Analysing the various types of intrusions one would find that there are generally three stages involved in targeting individuals or networks:

1. *The Acquisition Phase*: The first phase of a targeted attack usually involves an ''information acquisition phase'', in which information on potential targets is compiled from a variety of public sources, including social and professional networking sites, conference proceedings, academic papers and project information, in order to generate a profile of the target. This is an important phase because the ability to successfully compromise a target relies on more than just code designed to exploit vulnerabilities in software – it requires ''exploiting the human element'' as well. The digital traces individuals leave behind on the internet can be used to manipulate trust, and are used by attackers to encourage targets to execute malicious codes on their systems.
2. *Planting Malware*: Based on the information gathered, email lures are sent out to identified employees. These emails usually contain malicious attachments which help plant malware and also assist in probing the network of the organisation. This would enable the perpetrators to gather intelligence, get information of others in the organisation from contact lists, give access to sensitive files and documents, etc. The intelligence collected from these computer reconnaissance campaigns are also used for myriad of other purposes including identifying weak points in the networks, zero day vulnerabilities and also to plant trojans, vacuum Trojans,[2] botnets, etc. Once the malware has been planted the terminal becomes a zombie.
3. *Exploitation*: Once a network has been compromised then the actual process of exploitation starts which includes understanding how leaders think, the communication patterns between government agencies and private companies, and attaining valuable information stored throughout the networks.

Many organisations and individuals have already been subjected to the first and second stages of penetration but are not aware of the same.

The Contours of Cyber Security

Cyber-terrorism

According to the US Federal Bureau of Investigation (FBI), cyber-terrorism is any premeditated, politically motivated attack against information, computer

systems, computer programs, and data that results in violence against non-combatant targets by sub-national groups or clandestine agents. Unlike a nuisance virus or computer attack that results in denial of service, a cyber-terrorist attack would lead to physical violence or extreme financial harm. According to the US Commission of Critical Infrastructure Protection, possible cyber-terrorism targets include the banking industry, military installations, power plants, air traffic control centres, and water systems. Cyber-terrorism is sometimes referred to as electronic terrorism.

The threat of a cyber-attack is real and growing, as global and national systems become increasingly interlinked and interdependent. Indeed, speculation about the potential threat of cyber-attacks has been rife since the 1980s, and government systems across the world have been targeted from time to time by politically motivated, mischievous and state backed groups. Definitional disputes abound, and it is not clear how many of these can be described as cyber-terrorist attacks. Nevertheless, cyber technology has become a crucial tool in the terrorist arsenal, and its use to directly engineer widespread, and potentially life threatening, disruptions cannot be overestimated.

Cyber espionage

Two incidents readily come to one's mind: ghostnet and operation Shady RAT. The cyber-espionage ring named ghostnet was brought to light in March 2009 by the investigators Shishir Nagraja and Ross Anderson. In less than two years, the spying had infiltrated at least 1295 computers in 103 countries, including many belonging to embassies, foreign ministries and other government offices, as well as the Dalai Lama's Tibetan exile centres in India, Brussels, London and New York. This electronic infiltration gives an insight into the manner in which malware-based targeted electronic surveillance was carried out:[3]

1. First, it was a targeted surveillance attack designed to collect actionable intelligence for use by the police and security services, with potentially fatal consequences for those exposed.
2. Second, the *modus operandi* combined social phishing with high-grade malware. This combination of well-written malware with well-designed email lures, called social malware, was devastatingly effective.

Investigations documented how well-known crime-ware kits penetrated and extracted confidential material from the Tibetan community in exile in India, as well as the highest reaches of the Indian Ministry of Defence, Foreign Ministry, and its defence research establishment. The interesting features of this contour were that the perpetrators were inside the system for a long time but the hosts had no idea of their presence. The operations were as stealthy as could be imagined and were carried out simultaneously at many places. Not only was the data exfiltrated many emails were hijacked while in transit and amended or replaced with toxic ones as brought out in the report on the ghostnet. Though the operation was found to have originated in China, the Chinese government repudiated the allegations; the perpetrators were not identified and hence not brought to justice. Compare this to an espionage operation in the tangible world.

Operation Shady RAT

The operation was a series of cyber-attacks which started in mid-2006 and uncovered by McAfee in August 2011. McAfee dubbed the intrusions ''Operation Shady RAT'', with the acronym standing for ''Remote Access Tool''.[4] The attacks were said to have hit at least 72 organisations, including defence contractors, businesses worldwide, the United Nations (UN) and the International Olympic Committee. The McAfee report says the intruders were after data on sensitive US military systems, as well as material from satellite communications, electronics, and natural gas companies. Email lures containing an attachment sent to an individual with the right level of access at the company, and the attachment, when opened, triggered a download and installation of a malware. The malware created a backdoor communication channel to the command and control web server. This was quickly followed by live intruders jumping on to the infected machine and proceeding to quickly escalate privileges and move laterally within the organisation to establish new persistent footholds via additional compromised machines running the malware, as well as targeting for quick exfiltration of the key data they came for. The intruders were inside the system from at least 2006 to 2011 attacking different companies at different times. The type of data exfiltrated potentially pointed to a state actor, because there was no commercial benefit that could be earned from the hacks unless there was a nation-state customer.

Cyber Weapons

The reports over the last few weeks confirmed what was already known – that the Stuxnet worm had damaged a number of centrifuges in the Natanz Uranium enrichment facility. But the new discovery was that the attacks codenamed Olympic Games started under George Bush, expanded by Barrack Obama and were directly overseen by the White House. The second was the discovery of another worm ''Flame'' again directed against Iran and had been active at least since 2009. The discovery of these worms is a cause of concern because if nation-states start developing these type of worms the kind of attacks that can be launched become qualitatively different from what few hackers can do. The Stuxnet attack was an attack on the SCADA (Supervisory Control and Data Acquisition) system of the Iran's nuclear power plant at Natanz.

SCADA systems are notoriously insecure because they are designed to operate on an isolated network and offer security by obscurity. The Stuxnet worm took advantage of this and is supposed to have penetrated the system through USB drives. Once penetrated the systems are vulnerable, because they cannot differentiate between legitimate and malicious requests. In addition there is no built-in authentication process to protect the session from being hijacked.

Stuxnet is a sophisticated computer program designed to penetrate and establish control over remote systems in a quasi-autonomous fashion. It represents a new generation of ''fire-and-forget'' malware that can be aimed in cyberspace against selected targets. Those that Stuxnet targeted were insulated; in other words, they were not connected to the public internet and penetration required the use of intermediary devices such as USB sticks to gain access and establish control. Stuxnet has been described as a military-grade cyber missile that was used to launch an ''all-out cyber strike against the Iranian nuclear program''.[5] Using four ''zero-day vulnerabilities'' (vulnerabilities previously unknown, so that there has been no time to develop and distribute patches), the Stuxnet worm employed Siemens' default passwords to access Windows operating systems that run programmable logic controller (PLC) programs and manage industrial plants.

First Stuxnet hunted down frequency-converter drives which respond to the PLC computer commands that control the speed of the centrifuge motors. These drives are set at the very high speeds required by centrifuges to separate and concentrate the

uranium-235 isotope. Then Stuxnet alternated the frequency of the electrical current that powers the centrifuges, causing them to switch back and forth between high and low speeds at intervals for which the machines were not designed. Interfering with the speed of the motors sabotages the normal operation of the industrial control process. The worm contains a rootkit[6] that conceals commands downloaded from the Siemens systems and ensured that the display consoles projected the normal operating parameters.

On May 28, 2012, Kaspersky Labs announced they had uncovered a cyber-weapon even more powerful than Stuxnet. It was called Flame, and it made Stuxnet look like a practice run.[7] Once Flame infects a computer, it allows its creators not only to see every keystroke on the computer, but also – where the machine has a microphone and camera – to listen to any conversation and watch all activity in the vicinity of the computer. It can even access the Bluetooth capability of a laptop to steal data from other Bluetooth-enabled devices.

Botnets: Digital Foot Soldiers

Robots or simply bots, are software applications that run automated tasks over the internet. Typically, bots perform tasks that are both simple and structurally repetitive, at a much higher rate than would be possible for a human alone. The largest use of bots is in web search (*web spidering*) in which an automated script fetches, analyses and files information from web servers at many times the speed of a human. Each server can have a file, containing rules for the *spidering* of that server that the bot is supposed to obey. In addition to the uses outlined above, bots may also be implemented where a response speed faster than that of humans is required (e.g. gaming bots) or less commonly in situations where the emulation of a repetitive activity is required. However, bots have shot into prominence because of their notorious features. Bots are widely used to perform malicious activities ranging from information stealing to being used as a launching pad for distributed attack. Once a bot gets installed on a computer, the control of the machine passes on to a remote attacker and the terminal acts as per his commands. Such machines are popularly referred to as zombie machines or simply zombies.

A botnet is a network of compromised computers. A small botnet could consist of approximately 1000 computers. Typically a botnet of consists of a network of more than 10,000 computers. Several botnets have been found and removed from the

internet. The Dutch police found a 1.5 million node botnet[8] in October 2005 and disbanded it. In July 2010, the FBI arrested a 23-year old Slovenian said to have integrated an estimated 12 million computers into a botnet (called the Mariposa botnet). The network was used to steal passwords for websites and financial institutions. It stole computer users' credit card and bank account information, launched denial of service attacks, and spread viruses. Industry experts estimated the Mariposa botnet may have infected as many as 8 million to 12 million computers.[9] It has been estimated that botnets control up to 15% of computers worldwide that are connected to the internet.[10]

A bot army is a large, blunt instrument, but finding a bot on a computer can be a Herculean task, beyond the capabilities of some of the most internet-savvy people. Moreover, especially the Chinese, have started to make their bots ''user-friendly''. When bots were first introduced, they could slow down computer operating systems, eventually leading the computer user to reinstall the hard drive (and thus killing the bot). Sources say that Chinese bots now can be so efficient they actually make many computers run better by cleaning up the hard drive, trying to resolve conflicts and so on. They are like invisible computer housecleaners tidying up things and keeping users satisfied. Since there is no such thing as a free lunch the payment for this housekeeping, of course, is intelligence. This is a kind of information assurance form an alien system.

The Estonia Attacks

The attacks began on April 27, 2007, within hours of a war memorial's relocation by the Estonian authorities. The websites of the Estonian president, the prime minister, parliament and government ministries were quickly swamped with traffic, shutting them down. Hackers defaced other sites, putting, for instance, a Hitler moustache on the picture of Prime Minister Andrus Ansip on his political party's website. Suspecting the attacks to be originating from Russia, the Estonian government began blocking internet traffic from Russia on April 30 by filtering out all web addresses that ended in.ru.

By April 30 security experts noticed an increasing level of sophistication. Government websites and new targets, including media websites, came under attack from the electronic cudgel of botnets. When bots were turned loose on Estonia

roughly 1 million unwitting computers worldwide were employed. Officials said they traced bots to the United States, China, Vietnam, Egypt and Peru.

The next wave started on May 9, at midnight Moscow time, the day Russia celebrates victory in World War II. Four million packets of data per second, every second for 24 hours, bombarded a host of targets that day. By May 10, bots were probing for weaknesses in Estonian banks. The swarming bots almost paralysed the world's most digitised country. These botnets were part of an underground economy of crimeware kits and resources that are bought, sold and traded, and typically used for corporate warfare to knock political and business competitors off line.

Botnets also played a key role during the 2008 Russia–Georgia war, serving Moscow as a strategic multiplier for its military campaign through Distributed Denial of Service (DDoS) attacks. Commercial-grade botnets originating from Russian cyberspace silenced Georgian government websites and independent media, and disabled the government's ability to communicate to its population. The DDoS attacks helped create an information vacuum that paralysed Georgia's civil administration. In each case, Russia denied official involvement. Yet the botnet attacks directly supported Russian state policy. A genius of this strategy was that no one could link the Russian government and the cyber attackers, protecting the Russian state from political or legal culpability.

Cyber Fraud

Zero-day Vulnerability

A zero-day attack, also known as a zero-hour attack, takes advantage of computer vulnerabilities that do not currently have a solution.[11] This particular contour of cyber security could actually be the entry point for most intrusions for the elementary reason that they are unknown to anyone including the creators of the software. In most cases of a zero-day attack, malicious programmers take advantage of glitches in a software by finding them before the software's makers find them. A programmer can create a virus or worm that exploits the vulnerability and harms computer systems in a variety of ways. Typically, a software company will discover a bug or problem with a piece of software after it has been released and will offer a patch — another piece of software meant to fix the original issue. That is the reason why today we have so many updates and software patches streaming into our

systems. A zero-day attack will take advantage of the problem before a patch has been created. It is named zero-day because it occurs before the first day the vulnerability is known.

Not every zero-day attack truly occurs before software producers are aware of the vulnerability. Sometimes software producers learn of the vulnerability but developing a patch can take time. Alternatively, software producers may sometimes hold off on releasing the patch because they do not want to inundate customers with numerous individual updates. If the vulnerability is not particularly dangerous, software producers may choose to hold off until multiple updates are collected and release them together as a package. Still, this approach can potentially expose users to a zero-day attack. Now what if one has a pirated software version?

Several prominent security researchers have admitted selling previously undiscovered software vulnerabilities known as ''zero-days'' to defence contractors, who use these exploits to penetrate government and private networks or agencies. Some companies have built successful businesses by discovering security flaws in software such as operating systems and popular browsers like Google Chrome and Microsoft Internet Explorer, and then selling zero-day exploits to high-paying customers – which are often governments. Therefore there are many at present who are advocating that sales of zero-day glitches should be a key point in formulation of any cyber security policy formulation.[12]

On January 14, 2010, McAfee Labs identified a zero-day vulnerability in Microsoft Internet Explorer that was used as an entry point for Operation Aurora to exploit Google and at least 20 other companies.[13] Microsoft has since issued a security bulletin and patch but confessed that it knew of the glitch at least from October 2009. Operation Aurora was a coordinated attack which exploited the Microsoft Internet Explorer vulnerability to gain access into computer systems. This exploit was then extended to download and activate malware within the systems. The attack, which was initiated surreptitiously when targeted users accessed a malicious web page (likely because they believed it to be reputable), ultimately connected those computer systems to a remote server. That connection was used to steal company intellectual property and, according to Google, additionally gain access to user accounts. The ''highly sophisticated and targeted attacks'' – which Google said also affected 20 other large firms across a wide range of businesses – were traced to Chinese internet protocol (IP) addresses. These hacking attacks also involved

attempts to steal the search giant's intellectual property but the primary target appears to have been webmail accounts of Chinese human rights activists. A subsequent investigation revealed that the attack hit an additional 33 companies. The hackers sent targeted email messages to victims with malicious attachments which could take advantage of the vulnerability. These attacks are typically not detected by antivirus. The malware infected every user it could and obtained any contact information or any access information on the victim's computer to misrepresent itself as that victim. The aim was to drop a backdoor Trojan into compromised Windows machines and exfiltrate data.

Cross-site Scripting

Attackers use various methods to fool victims into visiting their phony website while pretending to be a trusted sender. Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser. Similar domain names, where an attacker will try to mimic the domain name by altering one letter, for example instead of www.yahoo.com an attacker would register yaho0.com. The last ''o'' is actually a zero, which would point to the attacker's website. An email might point towards a URL which exploits Cross-site scripting vulnerability on the service provider's website. Many banks have actually suffered such attacks. When an attacker gets a user's browser to execute his/her code, the code will run within the security context (or zone) of the hosting web site. With this level of privilege, the code has the ability to read, modify and transmit any sensitive data accessible by the browser. A cross-site scripted user could have his/her account hijacked (cookie theft), their browser redirected to another location, or possibly shown fraudulent content delivered by the web site they are visiting. Cross-site scripting attacks essentially compromise the trust relationship between a user and the web site. Applications utilising browser object instances which load content from the file system may execute code under the local machine zone allowing for system compromise.

In the case of the cross-site scripting attacks, it is the case that the service provider (unknowingly) becomes an accomplice to the attacker. The website location is authentic in the sense that it does belong to the legitimate owner, but the content of the website has been modified to harvest information such as usernames and passwords. The most straightforward and effective way for an attacker to launch his own code on his victim's computer is to actually attach his executable to an

email message. The most common of this kind of attack is known as ''Mass Mailing Worms'', like the Nimda worm which made rounds back in 2001, or the later variants of Bagle and Netsky worms which made up a substantial part of the email traffic during 2005. If one cannot easily verify the service provider's website against the one provided in the email, then it is generally very risky to click on the link in the email. Attackers will use various methods to fool victims into visiting their fake website while pretending to be a trusted sender.

Social Networking

This is an interesting concept which provides people a platform to get together virtually in real-time irrespective of the distances involved satisfying the basic need of human beings to stay together in groups. Today an estimated number of 1.5 billion people across the world have their profiles in social networking sites. These sites contain some seemingly innocuous but important personal details of the individual like preferences, hobbies, date of birth, places visited, education qualifications, email identities, etc. Social networking sites like Linkedln, Facebook, Orkut link individuals with their friends, family members, acquaintances and social circles. Photographs of all of these people are available – having been voluntarily submitted by the people themselves. The worldwide popularity of these sites extends to young and old alike, rich and poor, successful or impoverished. From simply an intelligence perspective, a high-ranking official a fugitive, drug dealer or criminal can be quickly linked to family and friends — intelligence that can point to their whereabouts, associates, the kind of assignments being performed and so on and to top this off one has access to high-resolution photos of everyone involved; an indispensable database by just spending few hours on the internet. This plethora of information is already being used by advertising agencies and nothing can stop them from being utilised by vested interests. India is the seventh largest market worldwide for social networking after the United States, China, Germany, Russian Federation, Brazil and the United Kingdom. Facebook has captured the top slot among social networking sites in India with 20.9 million visitors and growing.

At one end of the spectrum lies personal security which can be compromised. For instance the secret questions one has to answer for an online banking or an email account are most likely to be, what was your first telephone number? Your mother's maiden name? Your first school? And so on. Information of this nature are either

available on the site or can be obtained by ''intelligent chatting'' on these sites. Once the relevant information are obtained all one has to do is to log on to the target's account and click on the ''forgot password'' option!!! And answer the secret question and with a little luck one could have control of the account.

Whatever be the social networking site used one must be aware of emails that claim to be from these sites but are actually hoaxes and may contain ruinous content with the sole aim of obtaining usernames and passwords or the messages can even have an attached ZIP file containing a mass mailing worm, sufficient to cause damage to the computer and your reputation. Personnel from the armed forces, government officials, diplomats have already been subjected to these types of attacks.

At the other end of the spectrum are the events that have played out last year in the Middle East. In fact social networking websites had been used as a platform from which people made their political and economic grievances heard for a long time. However the Arab Spring brought the focus back on the social networking sites because of the speed with which the unrest spread. The uprising heavily relied on the internet, social media and technologies like Twitter, TwitPic, Facebook and YouTube in the early stages to accelerate social protest. There are even allegations that the US Central Intelligence Agency (CIA) was blindsided about the Egypt uprising by failing to follow developments on Twitter. Recognising the danger that social networks posed for the stability of its rule, the Egyptian government even resorted to blocking several social networking sites, but this had little effect since people found ways to go around the block.

Taking a cue from the Arab revolution the Pentagon is planning to monitor social networking sites for threats such as cyber-terrorism and to identify where a major event like the Arab revolution might next take place. The US Department of Defense is offering $42 million to fund research into monitoring social networks to track the formation, development and spread of ideas, and identify misinformation and attempts to foment unrest. The move by the Defence Advanced Research Projects Agency (DARPA) comes in the wake of use of social networks by insurgents in Afghanistan and Iraq and by home-grown threats such as Anonymous. The new proposals also seek to further efforts by the US government to automatically generate social media content through fake accounts, or bots. In March 2012 it was reported that US Central Command (Centcom) had awarded a contract to develop a software

that generates so-called "sock puppet" accounts – fake identities used to promote a particular view while concealing the user's true identity.[14]

China too has demonstrated that it is not very comfortable with the trends thrown up by social networking. The internal security apparatus of China is very conscious and sensitive to systems which have a tendency to promote any form of social unrest within its borders. A glimpse of this discomfort came to light during the uprising in the Middle East. The government pre-empted any local uprising by taking a proactive stance against even the small rumblings amongst the Chinese people. The Chinese authorities also promptly imposed strict controls on the media networking sites. Reporters and editors of major newspapers were instructed to use only reports disseminated by the official news agency Xinhua. Micro blogs were heavily censored while access to Facebook, Twitter, YouTube and LinkedIn were blocked. Censorship of the internet by China, known as the Great Firewall, was exhibited in the banning of foreign sites, such as Blogger and Voice of America, as well as a wide range of search terms and images the government deemed a threat to national security or counter-productive to the political party.

India's Vulnerability to Cyber-Attacks

Over the last decade, India has seen an increase in the number of cyber-attacks, from 2565 in 2008 to 8266 in 2009 to 10,315 in 2010. Ironically, one reason for the increase in the number of attacks has been the growing number of internet

Table 1. Cyber security incidents handled by cert-in.

Security incidents	2004	2005	2006	2007	2008	2009	2010
Phishing	3	101	339	392	604	374	508
Network scanning/probing	11	40	177	223	265	303	477
Virus/malicious code	5	95	19	358	408	596	1,817
Spam	—	—	—	—	305	285	981
Website compromise & malware propagation	—	—	—	—	835	6,548	6,344
Others	4	18	17	264	148	160	188
Total	23	254	552	1,237	2,565	8,266	10,315

Source: Cert-In (Indian Computer Emergency Response Team).

users here. Also, India's reputation as the back office of the West has attracted hackers looking to steal valuable data. However, most hackers and security experts agree that ignorance of cyber security is the most significant reason for India's vulnerability.

According to a Japanese security company *Trend Micro*, after targeting financial institutions in Europe and America, hackers are now increasingly targeting Indian financial institutions with the latest variants of malware like SpyEye and Zeus. An increasing number of phishing strikes are being reported from cities like Hyderabad, Nashik, New Delhi and Bangalore. This should not cause any surprise as in the past few years the detailed reports on the ghostnet, shadows in the clouds, the CWG (Common Wealth Games) report on the sale of tickets have clearly brought out India's susceptibility to cyber-attacks.

Foreign Worms

Even viruses that do not specifically target the Indian state, but originate abroad can then find their way here, can wreak havoc. Back in 2010, when the Stuxnet worm escaped Iran's nuclear premises and spread over the internet, it infected computers worldwide. India was the third-most affected country, with 8.31% computers affected, following Iran (58.85%) and Indonesia (18.22%).

Terrorist Use of Cyberspace: India

Cyber technology has played a vital role – albeit principally as a covert communication, propaganda or psychological warfare tool – in terrorist activities in India, for some time now. This includes prominent attacks in cities including Ahmedabad (2008), Jaipur (2008), Delhi (2011), Mumbai (2008) and Varanasi (2010), among others, over the past years.

Significantly, Lashkar-e-Toiba (LeT), the perpetrators of the November 26, 2008, Mumbai terrorist attacks (26/11), which claimed 166 lives, made substantial use of cyber technology in preparing and mounting the operation. The entire mission planning was done via Google Earth. The terrorists used cellular phone networks and social media to communicate with their command and control centres. The LeT also used voice-over internet protocol (VoIP) software to communicate with the 26/11 attackers on the ground and direct the large scale operation on a real-time basis. The distinguishing feature of VoIP-based communications, which form the technical

basis of popular communications software such as Skype and Vonage, is that audio signals are converted to data and travel through most of the internet infrastructure in binary, rather than audio, format, making them near impossible to detect and proactively intercept. The terrorists in the 26/11 attacks extensively used a VoIP connection provided by Callphonex a service provider based in New Jersey, United States. The money for this connection $250 was paid on October 27, 2008, through a MoneyGram Agent in Lahore. On November 25, 2008, a day before the attacks $229, the monthly rental, was wired to Callphonex through a Western Union money transfer agent in Brescia, Italy. The conspirators used the email ID kharak_telco@yahoo.com while communicating with Callphonex. This identity was accessed from IP addresses in Lahore, Chicago, Kuwait, Koroliov (Moscow region, Russia), Rawalpindi and Gulberg (Pakistan).

Investigations into Delhi, Varanasi, Jaipur blasts revealed that terrorists had hacked into unsecured wi-fi internet connections to send emails after the attack. After the Ahmedabad terror attack in July 2008, it was found that Indian Mujahideen (IM) activists had hacked into the unsecured wi-fi internet connection of an American national, Kenneth Haywood, residing in the Sanpada area of Navi Mumbai. An email claiming the attack was sent prior to the blasts from his IP address.

Investigations into the Varanasi (UP) blast of December 7, 2010, brought out that war-driving was used by IM to detect unsecured wi-fi networks. These networks were then used to send mails before attacks. (''War-driving'' is used to search for wi-fi wireless networks with the help of a laptop from a moving vehicle, in order to detect unsecured wi-fi internet points that may be exploited.)

The LeT has attained a significant degree of ''cyber efficiency'', and has been making increasing use of VoIP for communications. LeT started using VoIP as soon as the technology became common in the early 2000s. It was earlier possible to intercept telephone conversations or locate Lashkar cadres based on their IP addresses through their emails. But with LeT holding audio and video conferencing using over VoIP information gathering has become even more difficult.

Cyber crimes and the use of cyberspace and technologies by terrorists are, currently, at worst, powerful facilitators for terrorist groups. In the main, they remain marginal irritants to the system. Nevertheless, the potential threat they constitute is grave, and this has been noticed by the Indian state. A decision has been taken to

establish a National Cyber Coordination Centre, a fully fledged agency to counter this menace. However, current deficits in trained manpower and state of art equipment and infrastructure may hobble effective operationalisation for some time. A race is currently on, with terrorists, on the one hand, pushing the frontiers of cyberspace to harness the most disruptive of tools possible, and state agencies, on the other, seeking to interdict them in this enterprise. It remains to be seen which side in the conflict has the greater coherence and more sustained motivation.

After the 26/11 attacks, the Information Technology Act, 2000 has been amended by Information Technology (Amendment) Act, 2008 with effect from October 27, 2009. The amended act is a comprehensive act and provides legal framework and stringent punishment to fight all prevalent cyber crimes.

Policy for Cyber Infrastructure Protection

A detailed policy for national cyber infrastructure protection is presently before the National Security Council (NSC) awaiting its approval. The policy aims to identify all government agencies that would have a role in the protection of Indian cyber infrastructure and define their roles. This is not to just define their defensive roles but also to designate agencies for offensive roles.

According to the proposal CERT-IN (Computer Emergency Response Team India) would be responsible for protection of most of the cyberspace, while NTRO (National Technical Research Organisation) would be tasked to protect the critical infrastructure such as important government networks. NTRO would also be tasked to create the National Critical Information Infrastructure Protection Centre (NCIPC), which would be a command-and-control centre for monitoring critical infrastructure. It would be a round-the-clock centre, providing real time response to cyber security breaches. The proposal also envisages creation of sectoral CERTs in order to respond quickly to protect power distribution networks, Air Traffic Controls, traffic networks and other areas that are heavily dependent on networked systems, and thus are susceptible to attacks. The policy suggests that the defence forces would be responsible for their own networks' protection. NTRO and Intelligence Bureau (IB) would primarily be responsible for security of various government networks. While NTRO would operate through NCIPC, IB would be mainly looking at the physical security of networks. State police, CBI (Central Bureau of Investigation), National

Investigation Agency, etc., would be tasked to do follow up action, if any intrusions are detected.

Conclusion

The digital wars are here to stay and are a reality of this information age. The increasing interconnection of the world's computers, standardisation and homogeneity of communications protocols, programming interfaces, operating systems, computing hardware, and routers enable a single worm developed attack many systems. This provides attractive avenues for cyber attackers to exploit. Every new system comes with better and more secure components but at the user level it is not economical to replace the older ones. Therefore, the user demands of backward compatibility often means that older and less secure components are not replaced with newer components that reduce or mitigate the old vulnerabilities. The other problem is that systems are getting complex, elaborate spread is increasing exponentially, this implies that it will become progressively difficult to defend against or detect penetration. In addition to these today's cyber criminals are increasingly adept at gaining undetected access and maintaining a persistent, low-profile, long-term presence in IT environments. Moreover difficulties in identifying attackers, coupled with an uncertain legal and policy framework, make it more difficult to punish the offenders.

Therefore, one has to take proactive steps be vigilant and increase the cost of intrusions to keep unwanted visitors at bay. The cyber world is a world without barriers therefore artificial barriers have to be erected to prevent free ingress or egress. This is a world still in the nascent stages of its evolution, to stay ahead of the pack the leader will have to be imaginative and innovative.

Notes

1. A false positive occurs if there is a claim of a network intrusion but one did not occur. An Intrusion Detection System (IDS) analyses network traffic and raises alarms if it detects anything suspicious.
2. A vacuum trojan will extract information from a pen drive automatically when connected to a USB port.

3. ''Tracking Ghostnet: Investigating a Cyber Espionage Network,'' http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network (accessed March 2011).
4. Michael Joseph Gross, ''Operation Shady RAT—Unprecedented Cyber-espionage Campaign and Intellectual-Property Bonanza,'' *Vanity Fair*, August 2, 2011, http://www.vanityfair.com/culture/features/2011/09/operation-shady-rat-201109 (accessed March 2011).
5. James P. Farwell; Rafal Rohozinski, ''Stuxnet and the Future of Cyber War'', http://www.iiss.org/publications/survival/survival-2011/year-2011-issue-1/stuxnet-and-the-future-of-cyber-war/ (accessed Feb 2012).
6. A rootkit is a collection of tools (programs) that enable administrator-level access to a computer or computer network. Typically, a rootkit is installed on a computer after first obtaining user-level access, either by exploiting a known vulnerability or cracking a password. Once the rootkit is installed, it allows the attacker to mask intrusion and gain root or privileged access to the computer and, possibly, other machines on the network. A rootkit may consist of spyware and other programs that: monitor traffic and keystrokes; create a ''backdoor'' into the system for the hacker's use; alter log files; attack other machines on the network; and alter existing system tools to escape detection.
7. ''Powerful 'Flame' Cyber Weapon Found in Iran,'' *The Indian Express*, May 29, 2012 http://www.indianexpress.com/news/powerful-flame-cyber-weapon-found-in-iran/955204/0 (accessed June 2012).
8. Tom Sanders, ''Botnet Operation Controlled 1.5m PCs,'' October 21, 2005, http://www.v3.co.uk/v3-uk/news/1944019/botnet-operation-controlled-15m-pcs (accessed May 2011).
9. ''FBI, Slovenian and Spanish Police Arrest Mariposa Botnet Creator, Operators,'' FBI National Press Office, July 28, 2010, http://www.fbi.gov/news/pressrel/press-releases/fbi-slovenian-and-spanish-police-arrest-mariposa-botnet-creator-operators (accessed Dec 2011).
10. Ellen Messmer, ''The Botnet World is Booming,'' Network World, July 9, 2009. http://www.networkworld.com/news/2009/070909-botnets-increasing.html (accessed Jan 2011).
11. Marcia Hoffman and Trevor Timm, '''Zero-day' Exploit Sales Should be Key Point in Cybersecurity Debate,'' March 29, 2012, https://www.eff.org/deeplinks/2012/03/zero-day-exploit-sales-should-be-key-point-cybersecurity-debate (accessed May 2012).
12. Ibid.
13. McAfee, ''Operation Aurora,'' http://www.mcafee.com/us/threat-center/operation-aurora.aspx (accessed in May 2012).
14. James Ball, ''Pentagon to Monitor Social Networking Sites for Threats,'' *The Guardian*, August 3, 2011, http://www.guardian.co.uk/world/2011/aug/03/pentagon-monitor-social-networking-threats (accessed Feb 2012).