International Journal of Information Technology and Knowledge Management
January June 2009, Volume 2, No. 1, pp. 119-122

CYBER WARFARE – A GLOBAL THREAT

Gaurav Kumar

Many countries, including India are facing terrorism from many internal as well external forces. Terrorism should not be related with metallic weapons only but also related with the digital threats. Cyber warfare makes use of new type of armaments with various destructive effects on the target. Cyber weapons are usually programs with the objective to defend or attack a target. These digital weapons are freely available on the internet but some are kept private or are commercial. In Cyber warfare, there is no major difference between military and civilian infrastructure because non-military targets are also indirectly involved with military establishments. Disrupting the economy or damaging the public infrastructure can wield much larger effect as weapons of mass destruction and therefore it is necessary to build a strategy in order to get the global understanding of what attackers can do.

To ensure country's survivability, prosperity and stability, cyber warfare units have an important mission. There should be proper treatment to ensure national security and in worst case help with disaster recovery. Till now, countries relied on strength of conventional military units but now future of a country may depend on how well trained cyber warfare units and cyber-forensic experts are and how much expertise they have. Enemy is already there and ready to penetrate the strategic and economic infrastructure.

This article gives a view of the critical problem and its analysis.

Keywords: Cyber Warfare, Cyber Warfare Training, Cyber Threats, Cyber Warfare Arsenal, Cyber Terrorists, Digital Weapons, Cyber Combat

1. Introduction

Every country has full right to defend itself from any destructive force as well as attacking the enemy by all appropriate means. Cyber warfare is becoming more and more powerful on today's battlefield and affects development of armies in many countries as well as development of weapon technologies. Its use should not be underestimated as it is highly flexible and hard to detect. Its costs allow any country to train or hire a team capable of doing more than a complete army. Effective use of such teams can gain dominance on battlefield or force the enemy to retreat by shutting down its command infrastructure or communication network. Value of cyber warfare is growing and with digitization of conventional warfare technologies as well as using more complex devices creates risks and weaknesses that allow cyber warfare units to do more damage than they could in past.

Cyber warfare can be defined as use of IT equipment like computers, mobile phones or other IP enabled equipment to conduct a war via the internet. Cyber warfare is part of information warfare which involves collection of tactical information, spreading of propaganda or misinformation to demoralize the enemy and using information to overpower enemy systems, servers thus bringing normal life to a standstill. Various methods like DDOS, phishing, cyber vandalism, espionage, destroying critical utilities, and equipment failure come under cyber war. As per U.S. Army Cyber Operations and Cyber Terrorism Handbook 1.02, Cyber Warfare & Terrorism can be defined as "The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives. Or to intimidate any person in furtherance of such objectives."

It should be noted that China has tested an anti-satellite weapon last year with demonstration of the ability to destroy US satellites with the capability to "Blind" them by using lasers. China has launched 15 rockets and 17 satellites into space and still working on it. It is given in the very recent report of famous newspaper Guardian on November 20, 2008. China's ability to pursue cyber warfare is now "so sophisticated that the US may be unable to counteract or even detect the efforts", the report warns.

More than 140 countries around the world has developed cyber weapons for defense but lack a comprehensive doctrine and legal framework for responding to cyber attacks as well as using offensive cyber weapons against attackers and adversaries.

2. Cyber Warfare Arsenal

- Computer worms

* Computer Applications Department, Chitkara Institute of Engineering & Technology, Rajpura, Punjab, *E-mail: kumargaurav.in@gmail.com*

- Software vulnerability exploitation
- Denial of service attacks
- Info-blockades
- Root kits
- Botnets
- Malicious code
- Keyloggers
- IP spoofing
- Logic bombs and missiles
- Sniffing
- Spamming
- Trap doors
- Trojan horses
- Video morphing
- Carder
- Viruses

3. STAGES IN CYBER WAR

A full-fledged cyber attack may involve three steps.

(1) Breaking the transportation and control systems.

(2) Breaking the financial systems (stock markets, financial organizations and banks)

(3) Taking control of the nations' utilities.

A full-scale cyber attack can create panic among people and there may be the situation of emergency in all major establishments, be it Parliament, Rashtrapati Bhavan, major hospitals, schools or colleges. Any hacking attempt into the traffic light systems can cause havoc on roads in terms of accidents. A break into the IT systems controlling the metro rail services can cause disasters. A break into your bank's system or tax department can fish out your PAN Account, salary, the investments you have made, the assets you possess to the cars you own. Hacking your demat account can hurt you financially.

In the event of a full-fledged attack which brings down servers of critical public utilities or hands over their control to a rival party, recovery may take many days.

The CIA has also conformed that hackers had attacked IT systems last year causing a multi-city power failure. "We have information that cyber attacks have been used to disrupt power equipment in several regions outside the US. In at least one case, the disruption caused a power outage affecting multiple cities. We do not know who executed these attacks," Tom Donahue, a CIA senior analyst said at a conference in the US.

The US conducts various kinds of cyber War games on a regular basis including Cyber Storm II, (Annual Cyber War Game) with the focus on simulated attacks on IT, communications, airlines and energy sectors.

Major software development companies like Microsoft, Cisco, McAfee, Dow Chemicals participated in the war game which included US defense and intelligence agencies as well. The exercise cost about $6 million. No such large scale cyber war games happen in India. But private companies including Telcos and ISPs do conduct such drills.

As per India's CERT-In, in the year 2006, a total of 5,211 Indian websites were defaced, on an average of about 14 websites per day. Of the total number of sites that were hacked and defaced, an overwhelming majority were in the commercial domain (90 cases) followed by 26 in the .in domain. As many as 11 defacement incidents were also recorded in the .org domain. Of all hacking incidents in October, about 61 per cent related to phishing, 27 per cent to unauthorized scanning and 8 per cent to viruses/worms under the malicious code category. India, like the western countries has observed a massive rise in phishing attacks with incidents in 2006 which were 180 per cent higher than in 2005 and it is continuing.

Al Jazeera, a famous news channel has reported that China has developed such a sophisticated and active cyber warfare programme that the US "may be unable to counteract or even detect" an attack, a US congressional panel has warned.

The New York Times in December 2007 reported that in a series of "sophisticated attempts" against the U.S. nuclear weapons lab at Oak Ridge, Tennessee, Chinese hackers were able to "remove data." The story illustrates an alarming fact: China's cyber spies are now a part of America's computer network, literally.

As per reports, China's cyber warfare army is moving ahead, and India is also suffering. Over the past one and a half years, officials said, China has mounted almost daily attacks on Indian computer networks, both government and private, showing its intent and capability. The core of the attack is that the *Chinese Cyber Warfare Experts* are regularly scanning and mapping India's official networks. This gives them a very good idea of not only the content but also of how to disable the networks or distract them during a conflict. China is aggressively developing its power to promote cyber warfare and is now in a position to delay or disrupt the deployment of America's military forces around the world, potentially giving it the upper hand in any conflict, a panel of the US Congress has warned.

4. STRATEGIES TO FIGHT AGAINST THE CYBER ATTACKS

Recruitment of Experts

The investigating cyber attack team should be sent in escorted by Special Forces to investigate and neutralize

potential threat. Special Forces should be well equipped technically to secure the confidential data and neutralize any threats. They should ensure safety of cyber attack team and help them reaching the objectives of the training. The team should remain undetected by local authorities.

Cyber attack team should be composed of:

- Forensics specialists
- Firewalls specialist
- System security specialist
- Specialist in energy industry's applications security

Forensics specialists should be collecting any kind of evidence about the planned attack or possible future attacks as well as other information that might help increase the security of the homeland. The rest of cyber attack team should investigate possible threats seen from the local connections available to the attack group after the forensics specialists have recovered all the information necessary. In case they detect possible external automatic attack mechanisms the rest of the team should try to disable it and report them to the local defense teams of these external locations.

Logical Security

This is the main cyber-security battlefield where digital information is being exchanged or stored. Every security measure that is performed by a non-human device in the digital world is a member of this group.

There are many sub-fields here:

- Encryption
- Network security
- System security
- Application security
- Security monitoring/auditing

Training the Cyber Troops

Simply building cyber army from volunteers can't be a solution for national security even if they are the influential computer security experts. They may run fast or excel in precision shooting, but they will not succeed in logistics and tactics. In order to train a cyber army there needs to be a structure created that will use them efficiently. There have to be procedures created to help handle the situations effectively. All this needs to be built first before any training can begin. It is already clear that standard army field manuals can't be used to help build the cyber troops as here quality matters not quantity. Also tactics has to be built from scratch in order to achieve objectives necessary. Separation of offensive and defensive training is clearer and distinctive than in real combat training.

There are 3 Types of Training

(1) Proactive securing of a target

(2) Immediate reaction on an attack and security of the target

(3) Security forensics after attack and securing of target's infrastructure to prevent more attacks

Type 1: Training includes the deployment of a system with the applications of security checklists in order to bring the system and network components to a securely configured level. There are passive security measures deployed to monitor the system as well as provide sufficient auditing data to identify what happened.

Type 2: Training is analogous to security drills on a military base. Here, an alert is issued to team members have to gain control over the system and remove all the attackers from the system. It is done with cooperation with offensive warfare teams. After alert is issued there needs to be an escalation procedure executed which informs global security control center (GSC2) of an ongoing attack.

Type 3: Training takes place in systems which are already hacked. Its main objective is to analyze system state and logs and reconstruct the actions that attackers did. This can help to secure the system as well as give some information to offensive warfare teams how to perform similar attacks. Its objective is to detect what has been changed in the system to prevent further damage or fraud.

5. CONCLUSION

Cyber attacks are particularly dangerous because of the world's reliance on computers, networks and technology. These computers control critical systems that run power plants, telecommunications infrastructure, air traffic and more. Cyber attacks on banks, stock markets and other financial institutions could have a devastating economic effect on any country. With international law lagging in the area of cyber crime and cyber warfare, it resembles the early days of the wild-west (untamed territory).

Though the government has made arrangements to counter cyber warfare threats, a lot still needs to be done. For example, there are certain ways and means which one can use when e-mailing to avoid getting into the system and being tapped. There are certain brands of satellite phones which are difficult to tap, says Rajat Khare, Director of Appin Networks, a network security firm which maintains security for major establishments like the DMRC, Rashtrapati Bhavan etc.

Here, hiring the best talent can help. In a bid to counter cyber warfare the government has made a cyber warfare cell comprising 40 IITians. However, this is just a small step in building capability to counter cyber attacks.

According to Shamshad Ahmed, Regional Director, India & SAARC, Lumension Security (a network security provider), the third world war may be fought, if not entirely, then at least significantly, in the cyberspace. Apart from hostility on the ground, the enemy cyber warriors can bring down defense computer systems, all important government systems, they may blacken off data at the nuclear plants and introduce dangerous contaminants or malware which can destroy all communication links. India definitely needs an army of cyber warriors to confront the threat.

As India is touted widely as the IT superpower of the world, the Indian government, especially the cyber crime cells of Delhi Police and Ministry of IT, still doesn't have adequate talent to intercept the communication of terrorists via the internet. Lack of ability to attract good talent is an issue.

References

[1] Trojan Dragons: China's International Cyber Warriors, John J. Tkacik, Jr., (2007).

[2] Notes from a Presentation by Dr. Andrew Palowitch Entitled, "Cyber Warfare: Viable Component to the National Cyber Security Initiative?" at Georgetown University, November 27, 2007.

[3] Stephen Fidler, "Steep Rise in Hacking Attacks from China," The Financial Times, December 5, 2007, at www.ft.com/cms/s/0/c93e3ba2-a361-11dc-b229-0000779fd2ac.html. Source Cites Yuval Ben-Itzhak, Chief Technology Officer for Finjan, a Web Security Group based in San Jose, California.

[4] John Markoff, "China Link Suspected in Lab Hacking," The New York Times, (December 9, 2007).

[5] guardian.co.uk, Thursday (November 20, 2008).

[6] Indiapost.com, Monday, (January 12, 2008).

[7] Cyber War Gaps Loom, Colin Clark, (2008).