# Living With Cyber Surveillance and Espionage

**Colonel Sanjeev Relia@**

## Introduction

Surveillance and espionage have existed for time immemorial. While they were always a part of any military campaign and study, private lives of ordinary citizens were generally not much affected by such activities. Things are not the same anymore. With the internet invading into our lives like never before, we today live under constant surveillance of multiple agencies like the government, your employer and perhaps your friends and neighbours. While a lot has been written and spoken about surveillance using land, sea, air and space, not much is heard about the surveillance using the fifth domain – the cyber space.

In the age of internet, where information travels at the speed of light and events can be created in a matter of microseconds, privacy and safeguarding one's personal information has become a challenge. Securing private information was so much simpler when there was no internet. Today, Google perhaps knows more about what you do when, than you yourself know. The recent one minute video clip created by the social media Facebook for all its users clearly indicates that personal information is not as personal as we consider it to be and that someone is constantly watching over you.

## What are Cyber Surveillance and Cyber Espionage?

Surveillance is defined as monitoring of the behaviour, activities or other changing information, usually of people for the purpose of influencing, managing, directing, or protecting them.1 Technology has always played a very important part in such monitoring activities. In the realms of surveillance, the impact of networking technologies has been phenomenal which has given rise to a new model of surveillance called Cyber Surveillance.

Cyber surveillance is monitoring of computer activity, data stored on a hard drive, or being transferred over computer networks such as the Internet. Monitoring is often done clandestinely and may be done by or at the behest of governments, by corporations, criminal organisations, or individuals. It may or may not be legal and may or may not require authorisation from a court or other independent agency.2 In 2013, Edward Snowden, a former employee of the CIA and then a contractor working for the National Security Agency (NSA), revealed the scale of America's secret mass cyber surveillance programme at the transnational level codenamed "PRISM". (Interestingly Snowden is said to have learnt his hacking skills in an ethical hacking institute in India). Snowden's leaked documents uncovered the existence of a large number of global surveillance programmes, many of them run officially by the USA. While some called Snowden a hero for exposing the clandestine cyber activities of the Obama administration, there are some who also referred to him as a traitor. His disclosures nonetheless have fuelled global debates over mass cyber surveillance, government secrecy and the balance between national security and information privacy.

Cyber espionage on the other hand is the act or practice of obtaining secrets without the permission of the holder of the information (personal, sensitive, proprietary or of classified nature), from individuals, competitors, rivals, groups, governments and enemies for personal, economic, political or military advantage using methods on the Internet, networks or individual computers through the use of cracking techniques and malicious software.

## How is Cyber Surveillance/ Espionage Done?

The global surveillance industry is estimated to be growing at over 5 billion US dollar a year. Capabilities of surveillance technology have grown vastly in the past decade. Today, cyber surveillance technology ranges from malware which infects a target computer to record every keystroke, to systems for tapping undersea fibre-optic cables in order to monitor the communications of entire population. Some of the common surveillance techniques being used to gather information from the cyber domain are covered in the succeeding paras.

**Network Surveillance.** Majority of computer surveillance involves the monitoring of data and traffic while it is moving on the network. This includes both the Internet as well as stand alone discreet networks. The USA leads the pack of nations who indulge in such activities. While all phone calls and broadband internet traffic are required to be made available for real time monitoring under the Communication Assistance for Law Enforcement Act in the USA, international traffic moving on the internet too is susceptible to monitoring. Figure 1 below which was part of the secret PRISM presentation clearly indicates why any communication originated in India for a recipient in Africa or Europe can be easily tracked and monitored in the USA.3

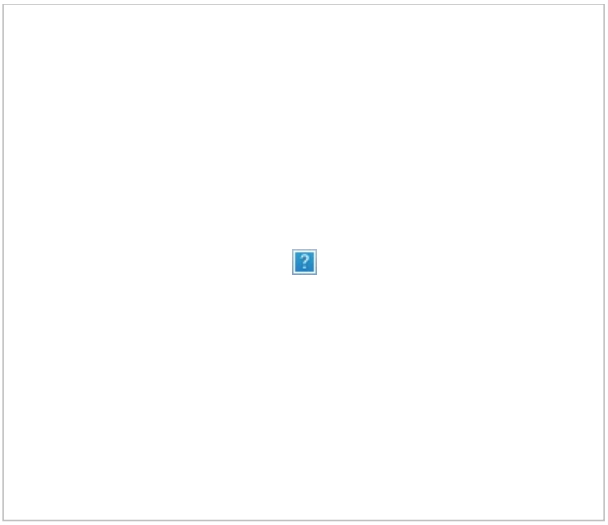

Figure 1 : International Internet Regional Bandwidth Capacity in 2011

As is clearly evident from the above diagram, bulk of the internet traffic flows via USA. Also, over eighty per cent of the servers and cloud providers are located in the USA. PRISM findings indicated that the internet service provider companies in the US whom the world trusted with their most private data were handing over the data to the NSA as if they too were a part of the entire clandestine operation.

**Packet Capture.** Packet capture or packet sniffing is monitoring of data traffic on a computer network. Data over the internet is transmitted by breaking it into small chunks called “packets”, which are routed through a network of computers. At destination, they are reassembled back into original message. Packet Capture Applications intercept these packets as they are travelling through the network, in order to examine their contents using analysis tools thereby deriving information out of them. As there is far too much of data travelling on the internet, automated Internet surveillance computers sift through the vast amount of intercepted Internet traffic to filter out information based on keywords or phrases, visiting certain types of websites, or communicating via e-mail or chat with a certain individual or group. Deep packet inspection (DPI) is the leading method of such surveillance. DPI technologies are capable of analysing the actual content of the traffic that is flowing. DPI allows network operators to scan the payload of IP packets as well as the header. This technique is often employed by law enforcement agencies and security forces trying to identify cyber criminals and cyber terrorists over the internet.

**Malicious Software.** Use of computer viruses, worms and Trojans is an effective method to examine or steal data stored on a computer’s hard drive, as well as to monitor activities of a person using the computer. A surveillance programme maliciously installed on a computer can search the contents of the hard drive for data, monitor computer use, collect passwords, and report back activities in real-time to its controller through the Internet connection. GhostNet a Trojan used by the Chinese in 2008-09 is an example of cyber surveillance of the Tibetans community in general and Dalai Lama in particular, using the internet. This Trojan allowed attackers to gain complete, real-time control of the infected machines and diverted the data to its controllers in island of Hainan. How deep routed is the Chinese cyber espionage set-up can be made out from Information Warfare Monitor (IWM) investigation detailed report of GhostNet, an extract of which is under :-4

> *“During the course of our research, we were informed of the following incident. A member of Drewla, a young woman, decided to return to her family village in Tibet after working for two years for Drewla. She was arrested at the Nepalese-Tibetan border and taken to a detention facility, where she was held incommunicado for two months. She was interrogated by Chinese intelligence personnel about her employment in Dharamsala. She denied having been politically active and insisted that she had gone to Dharamsala for studies. In response to this, the intelligence officers pulled out a dossier on her activities and presented her with full transcripts of her Internet chats over the years. They indicated that they were fully aware of, and were monitoring, the Drewla outreach initiative and that her colleagues were not welcome to return to Tibet. They then released her and she returned to her village.”*

**Social Network Analysis.** Social media technologies such as Facebook and Tweeter can be used by companies, marketers, and governments to collect significant amounts of data about individual users. Aim of this form of cyber surveillance is to create maps of social networks based on data from social networking sites as well as from traffic analysis information from phone call records. These social network “maps” are then data mined to extract useful information such as personal interests, friendships and affiliations, wants, beliefs, thoughts, and activities.

**Hardware Monitoring.** Today techniques exist where network or computer transmissions can be monitored using the hardware installed in the system. Some of these techniques are :–

(a) Monitoring by detecting the radiations emitted by the Cathode Ray Tube monitor. In the USA, surveillance using spurious transmissions being emitted by hardware is termed as TEMPEST.

(b) Using the transmissions between a computer and a presentation device such as a projection system.

(c) Picking up the noise of the key board clicking. Research shows that each key has a distinct noise which can be picked up using an audio surveillance device and the message deciphered.

(d) Use of the audio speakers connected to the system for picking up and transmitting information from a

computer.

(e) Radio Pathways. Tiny trans-receivers are built into Universal Serial Bus (USB) plugs and inserted into target computers which then communicate with a hidden relay station up to 12 kms away. This method is most effectively used for machines isolated from the internet.5

**Supply Chain Vulnerability.** A supply chain attack is an attack through subversion of hardware or software supply chain. A product, typically a device that performs encryption or secures transactions, is tampered with during manufacture or while it is still in the supply chain by persons with physical access. The tampering may, for example, install a root-kit or hardware-based spying components. The aim is to first gather information from the place where this hardware or software is installed and then to execute a cyber attack. Unless the user has facilities of test labs where such equipment and the software can be checked for spyware, a supply chain malware can never be detected. Countries like India where most of the public as well military hardware and software are imported remain vulnerable to supply chain surveillance and attacks. Although National Cyber Security Policy 2013 does talk of undertaking R&D programmes by the government for addressing all aspects including development of trustworthy systems, their testing, development and maintenance throughout their life cycle, is still a far fetched dream. It is unlikely that we will ever be able to sanitise hundred per cent hardware and software being used in the Country. But even if we are able to sanitise the critical components being installed in the national info-infrastructure, we would be able to save ourselves from loss of critical information and Stuxnet kind of attacks.

**Legal Cover to Surveillance in India**

The Economic Times in December 2013 reported that the Government of India will shortly launch 'Netra', the defence ministry's internet spy system that will be capable of detecting words like 'attack', 'bomb', 'blast' or 'kill' in a matter of seconds from reams of tweets, status updates, e-mails, instant messaging transcripts, internet calls, blogs and forums. The system will also be able to capture any dubious voice traffic passing through software such as Skype or Google Talk.6 The 'Netra' internet surveillance system has reportedly been developed by Centre for Artificial Intelligence & Robotics (CAIR), a laboratory under the DRDO.

So, does this mean that the Indian Government too has officially announced that all internet traffic in the country is liable to monitoring like the US Government did in PRISM? The Information Technology (IT) Act of 2000 and IT Act Amendment 2008 does give the power to the Government to carry out monitoring of the internet. Section 69(B) confers on the Central Government power to appoint any agency to monitor and collect traffic data or information generated, transmitted, received, or stored in any computer resource in order to enhance its cyber security and for identification, analysis, and prevention of intrusion or spread of computer contaminant in the country. Under this section, any government official or policeman can (or perhaps is already doing) listen in to all your phone calls, read your chats, SMSs and e-mails, and monitor the websites you visit. No search warrant from a magistrate is required to do so by them.

While the Act is a good tool to control cyber crime and cyber terrorism, Section 69(B) of the IT Act Amendment 2008 gives unrestrictive powers of the Government and law enforcement agencies in the Country which can be used to snoop upon unsuspecting citizens. Today the internet is a central element of the info-infrastructure of the information society and a global facility available to the public. The global and the open nature of the internet is a driving force in accelerating progress towards development in its various forms. It is, therefore, important to maintain an open environment that supports free flow of information across the globe and hence, it is essential that surveillance of such a resource, especially by nation states is dealt with caution.

Some governments across the globe argue that internet surveillance is necessary to ensure national security. As per them, keeping an eye on the data flowing over networks is a key to keep the nation safe. The unprecedented Chinese Government's programme of censorship of its people is an example of such a policy. The surveillance and content control system, launched in November 2000 by Peoples Republic of China, became known as the Great Firewall of China, where every bit of information flowing on the internet is kept under a watch by the Communist Government. There are also nations who feel that any such clandestine surveillance undertaken is a violation of human rights especially freedom of information. The stand of the Indian government is not too clear on this aspect. However, it is the duty of any democratically elected Government to appreciate that every law abiding citizen has the right to have a private life, a life which is not fully under constant surveillance of any state machinery.

**Impact of Cyber Surveillance and Espionage on the Society**

The Justice Department of the United States of America on 19 May 2014 filed unprecedented criminal charges against the members of the Chinese military, accusing them of economic espionage by hacking into the computers of US companies involved in nuclear energy, steel manufacturing and solar energy. Chinese government strongly rebuked the US over its claims of cyber-spying saying they were based on "fabricated facts" and would jeopardise US-China relations. Whether the charges are true or not, the fact of the matter is that cyber surveillance and espionage today has reached a level where it has started to impact bilateral relations between two strong nations.

The economic and business world suffers enormously form malicious cyber activities. While it will be difficult to gauge total cost to societies of cyber surveillance and espionage, but as a rough estimate as per a 2011 research, the upper limit of the cost of cyber espionage and crimes is somewhere between 0.5 per cent and one per cent of the national income. Also, not only does cyber espionage contributes towards high financial losses, it also has intangible loss component associated with it such as:

(a) The loss of intellectual property.

(b) The loss of sensitive business information (such as negotiating strategies), including possible stock market manipulation.

(c) Opportunity costs, including service disruptions, reduced trust online, the spending required in restoring any “lead” from military technology lost to hacking, and the realignment of economic activity as jobs flow out of “hacked’ companies.

(d) The additional cost of securing networks and expenditures to recover from cyber-attacks.

(e) Reputational damage to the hacked company.

Here is an example of how colossal damages can be inflicted to even a powerful nation like the USA through cyber espionage. As per a news report, a cyber espionage operation by China seven years ago resulted in stealing sensitive technology and aircraft secrets that have now been incorporated into the latest version of China’s new J-20 stealth fighter jet. The Chinese cyber spying against the Lockheed Martin F-35 Lightning II took place in 2007. Stolen data was obtained by a Chinese military unit called Technical Reconnaissance Bureau in the Chengdu province. The F-35 data theft was confirmed by the USA after some photographs of the J-20 were published on Chinese websites showing a newer version of the aircraft.7 The loss of critical design information of the F-35 was part of widening Chinese campaign of espionage against the US defence contractors and government agencies.

**Conclusion**

Invasion of the internet into our daily lives is a relatively recent phenomenon. Life is getting more and more dependent on the cyber world. Today the fear that surveillance can actually become so extensive as to threaten an individual’s healthy moral development is reasonable. Hence, the society needs to guard against it.

Most of the world is inadequately prepared for defending against these new types of surveillance and espionage techniques which have emerged in the last two decades. Governments, businesses, organisations, individual owners and users of cyberspace must assume responsibility for and take steps to enhance the security of the information technologies against such malicious cyber activities. Then only will this resource contribute towards positive growth of the society.

**Endnotes**


1. Lyon, David. 2007. Surveillance Studies: An Overview. Cambridge: Polity Press.

2. As available at http://en.wikipedia.org/wiki/Computer_and_network_ surveillance accessed on 30 Apr 2014.

3. So just what exactly is NSA’s PRISM by Rick Falkvinge as available at http://falkvinge.net/2013/06/08/so-just-exactly-what-is-nsas-prism-more-than-reprehensibly-evil/ accessed on 30 Apr 2014.

4. Tracking GhostNet: Investigating a Cyber Espionage Network, Information Warfare Monitor, 29 March 2009, available at http://www.nartv.org/mirror/ghostnet. pdf. Accessed on 30 Apr 2014.

5. NSA uses secret radio pathways to spy on offline PC’s, Times of India, 16 January 2014

6. Government to launch ‘Netra’ for internet surveillance, Kalyan Parbat, ET Bureau Dec 16, 2013 as available at http://articles.economictimes. indiatimes.com/ 2013-12-16/news/45256400_1_security-agencies. Accessed on 30 Apr 2014.

7. Top Gun takeover: Stolen F-35 secrets showing up in China’s stealth fighter, by Bill Gertz, Washington Times March 13, 2014.



**@Colonel Sanjeev Relia** was commissioned into the Corps of Signals on 20 Dec 1986. Presently, he is a Senior Research Fellow at the Centre for Strategic Studies and Simulation, United Service Institution of India, New Delhi.



Journal of the United Service Institution of India, Vol. CXLIV, No. 596, April-June 2014.