Chapter 12

HOW MASQUERADERS INFILTRATE A SYSTEM

INTRODUCTION

As a sequel to the phenomenal expansion of cyberspace, growth of information technology in its varied facets and coming of age of e-civilization, new challenges have been thrown up, particularly with regard to policing the Internet; profiling cyber terrorists and criminals; and, privacy of the citizens [5]. Cyber surveillance has assumed importance in the context of the rampant misuse and abuse of the Internet; unauthorized access to data; forgery of digital signatures; infringement of intellectual property rights covering patents and trademarks; fraudulent subversion of electronic payment systems; wars over domain names; browsers and portals; and, a growing menace of intruders, masqueraders, and saboteurs [1].

This chapter deals with a broad sweep of technologies and issues connected with policing, profiling and privacy as applicable to cyber surveillance and the infiltration of masqueraders. Presently, there is a perceptible bias against technology and technologists becaU.S.e the decision-makers are of the generalist hue and, exceptions notwithstanding, pride themselves on technological indifference. Therefore terms, which are everyday vocabulary elsewhere and the forte of terrorists in their application and exploitation, are foreign to most of U.S. This chapter is not a primer, but its rationale and thrust would be lost if technologies and methodologies used for policing cyberspace of:

- Packet-sniffing bots
- E-mail forgery
- Carnivore
- Omnivore
- Black bag jobs
- Pen register
- Trap and trace
- Intrusion detection system
- Creating effective and responsive databank
- Global Information Base (GIB)

- Knowledge-Aided Retrieval in Activity Context (KARNAC)
- "Junglee"
- The fail-proof and foolproof system for sifting, archiving, and mining data for profiling of terrorists, hackers, and criminals [1]

are not understood [1].

Does the government have powers only to investigate cyber offenses after these are committed and be unmindful of preventing crime is the moot question that you must ask yourselves before castigating the authority. This chapter also discusses the security versus privacy and legality issues of wiretapping; and, the laws of other countries of interest. It is the burden of this chapter that privacy comes a poor third in the hierarchy of reckoning after social welfare and security. Security flows from eternal surveillance, so get a good radar and keep it sweeping [1]!

PREPARING FOR THE NEW WORLD ORDER

It was way back in the 1960s that the U.S. strategic think tank, Rand Corporation, did some serious. thinking on the U.S. command-and-control setup in a nuclear scenario and how the U.S. authorities could communicate after the first nuclear strike. A dilemma that confronted them was that post-nuclear America would need a C3 (command, control and communications) network, linking city-to-city, state-to-state and base-to-base. A nuclear attack would render any conceivable network in tatters, no matter how meticulous the planning for network protection was to make it nuclear and EMP proof. Baffled by the problem of control, the Rand Corporation discarded the concept of centralized authority over the network on the reasoning that such a network would be the first to be targeted and eliminated by an enemy missile attack [1].

In a highly secret meeting, Rand came out with a novel and bold solution, perhaps a wicked one, too. It suggested, let there be no central authority, assume the network to be vulnerable at all times; design the network from the very beginning to operate while in tatters, and perhaps with tongue in cheek, let the friends and allies share the electronic vulnerability and also feel the pinch [1].

More than 42 years later, there is no central authority over the Internet, the network is bare and exposed to its marrow, continues to be in tatters and its vulnerabilities, though it be of a different kind, are a concern of the entire civilized world. It is a paradise for masqueraders, criminals, terrorists and anarchists [1].

Let U.S. shed crass naiveté. The Internet was an instrument of the Cold War and still figures high in U.S. security concerns. It was created to serve Uncle Sam's globalization agenda, more of the info-dominance and less than any humane munificence. Its roots are in ARPANET. ARPA stands for Advanced Research Projects Agency, which is part of the U.S. Department of Defense. One of the goals of ARPANET was research in distributed computer systems for military purposes. The emphasis is deliberately on military purposes, because that is how the Internet in its infancy bore a hierarchical structure [1].

Cyberspace has become the new arena to masquerade, show muscle, peddle crime, terrorism, and even anarchism. You now face the roughs and the menace of new kinds of

wars with hitherto unparalleled diversity, intensity and perversity, like domain wars, portal wars, content wars, flame wars, hacker wars, cyber wars and ironically wars of endies, reminding the U.S. of the holy wars of yore. These have sharpened the bite of familiar conventional, unconventional and proxy wars. Then there are the less-abuses of the likes of spying, spoofing, sniffing, spinning (spin doctoring), spamming, stalking, sleazing and seeding (viruses, worms and Trojans). The technologies are converging and unifying the techniques and the artifacts; the societies are diverging and dividing the humans; herein lies the rub, and the intra-conflict of e-civilization [1].

Let there be no doubt that Chinese and U.S. think-tanks take their homework seriously. Both nourish the perception that the Internet provides the chance to dominate the rest of the world through means other than the military. The Internet is the high ground and a first-termer at the National Defense Academy will know that in tactics the first lesson that one learns is to occupy the high ground and hold it under all costs [1].

The new world-disorder is the most apparent, yet least talked of, consequence of the technology marvel – call it the anti-marvel of the day. The very paradigm shifts in the defining technologies of the last decade have been very rapid, accelerating, and penetrating, as has been their wont. Perspectives on revolution in military affairs and ipso facto e-civilization are in a flux; so are the dynamics of political, social, and economic sinews that interplay [1].

Till the 9/11 terrorist attack, the U.S. had unchallenged supremacy over the Internet, its projection of credentials, the prime virtues of universality of access and equitable stake-holding, notwithstanding. The information-coordinated, cyber-enabled terrorist attacks on the World Trade Center, the Pentagon, and the aborted one on the White House simply shattered this facade of supremacy. Among the many nagging questions that have confronted the U.S. authorities in the wake of 9/11 is, what precisely was the nature of support that cyber access lent the terrorists? And, what could be done to plug those holes, and what steps should be taken on the cyber front to prevent recurrence of this kind of tragedy? Could government's increased use of cyber-surveillance technologies have helped [1]?

The art of cyber-snooping and packet-sniffing has reached such an acme of sophistication that nothing is hidden from prying eyes, be these of law enforcement community, be these of hostile intelligence agencies, or even terrorists and criminals. Technologies exist that allow intelligence or counter-intelligence to eavesdrop on voice and electronic communications. This also includes 10 sniff e-mails; matching peoples' faces with those in a database as they pass by cameras; and, voice-analyzer tapes, as they are played on al Jazeera. Or, to capture keystrokes as they are punched in a PC. You have then, metaphorically, a network of eyes in the sky satellites that view the opponent's turf with amazingly high-resolution cameras [1].

The new world-disorder has unabashedly compromised the Intellectual Property Regime (IPR), and intensified technology denial and counter proliferation regimes. It would be naive to be dismissive in the adverse of influence, like infringement of sovereignty and information apartheid, that it would inevitably entail. Then there are other exploitative policies like bias towards capitalism, monopoly, concentration of content, discriminatory standards, patent regimes, copyrights and sui generis databases, besides application of U.S. domestic laws on other countries in respect of regulatory, privacy and security issues. New terms have been

coined (domainism, which implies prejudice on the basis of Internet address and infra dig commercial online credentials) [1].

Cyber Terrorism

What is terrorism? Is cyber terrorism a hype or for real? What incidents have happened so far that impact security in cyberspace? What is likely to happen in the future? And what lessons can you draw from the cyber-enabled terrorism targeted against you and other countries and societies, not forgetting that the threat is often the laptop for attack [1].

According to the National Information Protection Center (NIPC), Cyber terrorism is an act through computers that results in violence, death and/or destruction and creates terror for the purpose of coercing a government to change its policies. A little differently worded definition from the FBI states, Cyber terrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data, which results in violence against noncombatant targets by sub national groups or clandestine agents. Both of the definitions talk of violence, death and destruction, but the blow and brunt of cyber terrorism are more psychological than physical [1].

Cyber terrorism is the cheapest way of hacking belief systems, and destroying data that supports them. It is the most ubiquitous. way of hacking the cerebrum at the individual level, psyche at the collective level, and inducing fear. It's what's also now termed as waging cognitive war on the one hand; and, on the other hand, denial of service attacks and mass mailing malicious codes, worms and virus, of the Sobing and Bugbear variety that eat the vitals of cyber systems. Cyber anarchy is a vested interest. It is a veritable psychological war zoom that promotes and spreads syndromes. The impact of Anthrax, SARS and Melissa is more psychological than physical. So is that of cyber infraction. It creates paralysis and dysfunction in decision-making [1].

Terrorists have taken to cyberspace like fish to water. They use it to manage a worldwide Internet enabled terror information infrastructure (InfoInfra). They also:

- Issue terror threats
- Conduct propaganda and psychological operations
- Communicate through e-mail-enabled crypto, stegano, and PGP (Pretty Good Privacy) messages
- Launder money (the most popular of which is hawala operations)
- Obtain WMD (weapons of mass destruction) intelligence
- Carry out technology snooping
- Make contacts with hackers, crackers, and criminals
- Plan proxy operations
- Transact, shop, and schedule covert supplies of contrabands, drugs and weapons
- Arrange clandestine meetings and RVs through ICQ (the acronym stands for "I seek you"), IRC (Internet Relay Chats) and for postings on bulletin boards in short what constitutes the jugular vein of terror [1].

Cyber terrorism has emerged as the most potent threat vector. It has prospered under the tutelage of hacking. In the past, motives were political, socio-religious, and even anarchical

and the acts are pulled off in such a way that the perpetrators hogged maximum publicity. Now, the motives remain much the same but the execution has become exceedingly typified by anonymity. The cyberspace is a delight for hacking, more so for anonymous and remote-controlled surreptitious operations. It is because both the perpetrator and the victim deny the impact if not the criminal or terror act, and the former to repeat the modus operandi and the latter to conceal the shame and economic consequences of being cuckolded [1].

Asymmetric warfare anchors on the unpredictable, the unknown unknown. And, cyberspace lends it the environment to execute and coordinate through remoteness and randomness, yet unbelievable but true, with synchronization bordering on precision. Scenarios are aplenty, varied and beyond the much touted war-gaming. Consider for instance a virtual attack coinciding with the real one; imagine mayhem if Code Red and 9/11 were mounted simultaneously [1].

The two most serious consequences of cyber terrorism are threats to critical infrastructure and loss of sensitive data. The infrastructure threat is to the cybernated and computerized systems of railways, dams, hospitals, oil pipelines, TV and AIR stations, telecommunications, air traffic, or any other networked system. Although this is most potent of the cyber attacks, one tends to dismiss it as the least probability. Even in the U.S. and that too after 9/11, the threat has been downplayed. For example, the Massachusetts Water Source Authority indicates that cyber terrorism to them is a lower-level threat. And, this is despite the fact that hacker, Vitek Borden, succeeded in releasing one million gallons of sewage into the water supply in Australia. He was at it for years, and that he had made 44 previous attempts that remained undetected, is a telling account of concern for cyber surveillance [1].

Compromising critical computer systems to steal or irreversibly damage vital data is the second objective of cyber terrorism. The vulnerable targets are ministries, nuclear establishments, military, R&D, defense production and other sensitive data. The greater the criticality of data, the more vulnerable it is [1].

Before closing the discussion on cyber terrorism, it would be prudent to remember that terror is a psychological condition. To succeed, it has to be communicated. The key to winning war against terror is to disrupt the terrorist's communications and protect your own. The gurumantra is to keep them under electronic cyber surveillance, wireless, cellular [4], short message service (SMS), and to ferret out terrorist information signatures before they strike. This is called "Total Information Awareness," although the term is shrouded in secrecy and has invited the wrath of privacy groups [1].

Cyber Surveillance

Cyber surveillance could be defined as a systematic observation of cyberspace by surfing, sniffing, and snooping. Or, by other means, with a view to locating, identifying, determining, profiling, and analyzing, by all available and predictable means the transmission of e-mail, movement of packets, file transfer, e-money transactions and subversive activities of criminals, cyber terrorists, hostile regimes and intelligence agencies. It equally applies to watching over friendly elements to anticipate and prevent cyber crime and social abuse, carry out counter surveillance, and find holes in our own procedures and systems of cyber security [1].

Cyberspace attacks mounted by different actors are indistinguishable from each other, in so far as the perceptions of the target personnel are concerned. In this cyberspace world, the distinction between crime and warfare is blurred. This blurring between crime and warfare also blurs the distinction between police responsibilities to protect societal interests from criminal acts in cyberspace, and military responsibilities to protect societal interests from acts of war in cyberspace. A corollary to this is the undefined division of the responsibility of conducting cyber surveillance between the security forces, like the:

- Military, paramilitary and police
- The intelligence and investigative agencies like RAW, IB, CBI and those of the three services
- Between private and public sectors
- A host of other divides that dare and defy the divide-less cyberspace [1].

CHINESE CHECKERS

A complete chapter has been devoted to China's exploitative presence and forays in cyberspace in Yashwant Deva's Secure or Perish. Since then, the Chinese have come a long way and PLA's capabilities to spy in cyberspace are next only to Echelon and their capabilities to wage cyber war and protect their cyber assets next only to NATO [1].

The scope of Chinese Information warfare spreads over a wide canvas – military, social, economic and political, and encompasses electronic warfare attacks, tactical deception, strategic deterrence, propaganda warfare, psychological warfare, network warfare, structural sabotage, and trade warfare [2]. And, of greater significance, attacks on human cognitive systems. Much stress is laid on the last two, besides network security and offensive and defensive maneuvers. The Chinese have no compunctions whatsoever about employing dubious tactics, machinations, and subterfuge such as, invasion of adversaries' financial systems through the use of computer viruses or human sabotage, disrupting enemies' economies, or spreading rumors over the Internet and thus psychologically impacting society [1].

China has an unparalleled experience in fighting cyber wars, first against Taiwan in 1999 when Web sites on either side of Taiwan Strait became high-tech battlegrounds in a new kind of conflict. And then, against the U.S. in April to May of 2001. It is believed that during the cyber dueling with Taiwan, the Americans were helping the Taiwanese and testing their own systems of cyber attacks developed by the Pentagon to penetrate enemy networks in time of war [1].

In July 1999, China's Liberation Army Daily indicated that the country needs to go all out to develop high-quality Internet warriors. It exhorted that this warrior community should include human resource development in exclusive universities, as well as work on attracting some private computer aces to take part in Internet combat. A follow-up chapter warned of breaches in Chinese computer security: The wolf has already come. Pick up your hunting rifle [1]!

The most serious attack has been that of the Chernobyl virus., written by a Taiwanese computer-engineering student, Chen Ing-hao. The virus, released on the Internet in 1998,

lay dormant until April 26, 2003, when it got activated and wreaked havoc on computers around the globe. It reportedly impaired 360,000 computers in China and caused damage of up to $120 million, according to the official New China News Agency. Whereas China accused Taiwan of complicity, the Taiwanese authorities maintained that it was an individual act of crime. The Guaangzhou Military Region, which includes the South China Sea Fleet and the Second Artillery units, was hit with a computer virus throughout its entire network, linking 85 strategic and combat bases. In the morning hours of April 26, 2003, the entire system was paralyzed. The Central Military Commission and the Headquarters of the General Staff had no alternative but to declare a state of emergency in order to mobilize the command system and military defenses. At the same time, Jiang Zemin immediately signed an emergency order placing the Nanjing Military Region and the East China Sea Fleet on second-degree combat readiness. This was the first time China's military entered a second degree combat readiness since the death of Deng Xiaoping in February 1997. According to an internal military announcement, it was discovered that computer operations of the Chinese Central Command had been severely disrupted. After the incident, the State Council and the Central Committee Military Commission promptly ordered the formation of a task force composed of the General staff Intelligence Department; General staff Technology and Communications Department; Ministry of Defense Technological Intelligence Department; Institute of Military Sciences' Special Technologies Department (also known as Department 553); and, the Ministry of Security's Security Bureau. Later, this task force prepared detailed plans to cripple the civilian information infrastructures and financial banking, electrical supply, water, sewage, and telecom networks of Taiwan, U.S., India, Japan and South Korea – should the need so arise [1].

The Chinese take training in information warfare very seriously. The PLA has conducted several field exercises in recent years. An informaticised people's warfare network simulation exercise was conducted in the Echeng district of Hubei province. Five hundred soldiers simulated cyber-attacks on the cybernated infrastructures of the likely adversaries. In another exercise in the Xian in Jinan Military Region, rehearsals were carried out in planting information mines; conducting information reconnaissance; changing network data; releasing information bombs; dumping information garbage; disseminating propaganda; applying information deception; releasing clone information; organizing information defense; and establishing network spy stations. The macabre prospects and scary reach of these preparations should spur you to action, should you be on the wrong side of the Chinese bludgeon [1].

INTERCEPTION

Almost all types of electronic communications can be intercepted and that, too, without much expertise or expensive equipment. Surveillance hardware and software are not difficult to access. The former are available in many electronic stores across the globe and the latter easily downloadable for the asking. Even LTTE had a string of electronic workshops along the eastern coastline where they were making radio controlled Improvised Explosive Devices (IEDs), bugs, and other such gadgetry [1].

Most of the world's Internet capacity lies within the U.S. or connects to the U.S. Communications in 'cyberspace' normally travel via the United States, or through intermediate sites within the U.S. The traffic is broken into packets and routes taken by each depend on the origin and destination of the data, the systems through which it enters and leaves the Internet, and a myriad other factors including time of day. Even short distance traffic, say from New Delhi to Chennai, may travel via routers and Internet exchanges in California or elsewhere in the U.S. It, therefore, follows that a large proportion of international and domestic communications is readily accessible to the National Security Agency (NSA), so that it can listen to telephone conversations of its own citizens; as well as, those of other countries. So, what's in skip zone, is also covered by the other partners of Echelon [1].

For readers not familiar with Echelon, it is the name given to the global electronic surveillance system in which five partners cooperate, like NSA of the U.S., General Communication Headquarters of the UK, Communications Security Establishment (CSE) of Canada, Defense Signals Directorate (DSD) of Australia and the Government Communications Security Bureau of New Zealand. It sits between the world's well-known information and wild paranoid speculation. On one hand, you know that the NSA's mission is electronic surveillance. On the other hand, you don't know how far the abilities of NSA extend. The NSA is forbidden by law from conducting surveillance within the United States; but, it violates the law anyway, due to the arrogance and complete disregard for the law by the Bush administration. In theory, it is also not allowed to monitor the activities of U.S. citizens abroad; but again, all new passports now have a RFID chip (radio frequency identification chip) embedded within them (see sidebar, "Hacking With RFID Tags"), which allows the NSA to monitor its own citizens abroad. Can you smell "1984's" Big Brother anywhere?

Hacking With RFID Tags

Hackers can use RFID tags to infect the middleware and back-end databases that power RFID systems with worms and viruses, researchers recently found. RFID tags provide a conduit for exploiting back-end systems with buffer overflows, malicious code and bogus SQL commands. RFID applications that use Web protocols to query back-end databases could even be susceptible to the same types of security exploits as Web browsers. The potential for RFID viruses will cause developers to be more cautious in the design and implementations of RFID systems.

A lot of RFID deployments are highly proprietary, so open systems would seem to pose the most interesting targets for hackers. The key to avoiding RFID exploits is to modify RFID database processing code to ensure the integrity of data that's passed from the tag to the back-end database. When only valid data is passed through to the database itself, there should be no concern for SQL or buffer overflow or similar attacks.

While VARs indicate that they see the potential for RFID-based attacks, there is some disagreement. RFID tags don't operate on software and don't have executable code, which means it's not possible to infect them with viruses.

The notion of programming a virus into an RFID tag also is impossible due to storage limitations. You can't build an executable code out of 96 bits.

However, the small memory space of an RFID tag as a barrier to the future development of RFID viruses doesn't seem to exist at this time. It's surprising that any vendors dismissed the possibility of RFID viruses by indicating that the amount of memory in the tags is too small.

It is therefore recommended that developers of the wide variety of RFID-enhanced systems take steps to add stronger security to limit the potential damage from the coming wave of hackers experimenting with RFID exploits, RFID worms and RFID viruses on a larger scale. Research on RFID viruses is important because it highlights the importance of designing future architectures for RFID systems that can analyze data and filter out malicious code. As this technology evolves, you need to keep in mind that more complex tags need to have strong security features and protocols [3].

Today, the Bush administration is spying on all Americans full time. However, there was a time in the not too distant past that allowed NSA to have (and still has) extensive exchange agreements that are mutually convenient to overcome the legalities. For example, there is an agreement where the UK spies upon the U.S., and then shares with the NSA some of the information it gathers. In the past, even though the NSA was unable to legally spy on Americans, it could still can get intelligence on Americans through this exchange agreement. It is widely accepted that the NSA and the National Reconnaissance Office (NRO) operate surveillance satellites, including those for electronic surveillance as well as photographing the earth's surface. These satellites can monitor terrestrial microwave as well as cell-phone traffic. The NSA, likewise, has numerous ground stations spread throughout the world (the NSA operates one in communist China for the purpose of monitoring Russian activities. The party line of the Civil Libertarians indicates that the Echelon system is a whole new critter; it doesn't monitor the communications of the post-Soviet purveyors of glow-in-the-dark explosives; nope, the Echelon system keeps an eye on everybody [1].

In 2006, it was estimated that the amount of Internet traffic flowing through cables beneath the Atlantic was roughly 1,200 gigabits/second. While this is 70 million times faster than a dialup connection, it is well within the range and capability of the NSA to intercept. In the same year, the company Network ICE was selling Internet monitoring equipment where a single machine costing roughly $25,000 to run its software could monitor roughly 7-gigabit/second. This means that the NSA has acquired the ability to monitor all cross-Atlantic traffic with a small investment of only $70-million in hardware [1].

Packets or data grams include numbers that represent their origin and their destination, called IP addresses, which are unique to each computer. Therefore, tracing them is not difficult at all. Handling, sorting and routing millions of such packets each second is

fundamental to the operation of major Internet centers. The same facilities and processes could be used for interception too. Internet traffic can be accessed either from international communications links entering the U.S., or when it reaches major Internet exchanges. Both methods have advantages. Access to communications systems is likely to remain clandestine – whereas access to Internet exchanges might be more detectable, but provides easier access to more data and simpler sorting methods [1].

Technologies And Methodologies

New technologies (packet sniffers, computerized voice recognition and keystroke biometrics that can automate surveillance) are being actively developed by many countries, both of the West and the East. A packet sniffer is a wiretap device that plugs into a computer network and eavesdrops on the network traffic. Like a telephone wiretap that allows an intelligence agency to listen in on conversations, a sniffer program lets someone listen in on computer conversation. Carnivore is one such packet sniffer or packet filter. According to a former employee, NSA had, by 1995, installed sniffer software to collect such traffic at nine major Internet exchange points (IXPs) [1].

Equipment for covert collection is highly specialized, selective and miniaturized. One major NSA supplier "The IDEAS Operation" now offers micro-miniature digital receivers, which can simultaneously process Sigint (Signal Intelligence) data from eight independent channels. This radio receiver is the size of a credit card. It fits in a standard laptop computer. IDEAS claim, reasonably, that their tiny card performs functions that would have taken a rack full of equipment not long ago [1].

The Ottawa Citizen reported that CSE had spent over $1.1 million to 'isolate key words and phrases from the millions of signals to create a speaker identification system. A joint NSA/CIA "Special Collection Service" manufactures equipment and trains personnel for covert collection activities. One major device is a suitcase-sized computer processing system, called Oratory. It is, in effect, a miniaturized version of the Dictionary system, capable of selecting non-verbal communications of interest from a wide range of inputs, according to pre-programmed selection criteria [1].

The amount of information monitored by the NSA is huge; for it's processing, the NSA uses a keyword dictionary. Massive supercomputers sift through the traffic looking for these keywords. These dictionaries are updated almost daily according to world conditions. Dictionary sorting and selection can be compared to using search engines, which select Web pages containing key words or terms and specifying relationships. The forwarding function of the Dictionary computers may be compared to e-mail. When requested, the system provides lists of communications matching each criterion for review, analysis, gisting or forwarding. It may be a wild speculation, but is possible that al-Qaeda could have rigged up a Dictionary of their own. How else is it possible to keep track of so much intelligence today that they exhibit without much ado, and without being afflicted by a zero-error syndrome [1].

Although the term black-bag operation has originated in the U.S. and specific to their context, intelligence agencies the world over have taken to it and widely use it. It is a secret break-in by a law-enforcement or intelligence organization. In other words, it is designed to secretly search the location, copying files or other materials, and to plant bugs, wiretaps, or

key-loggers. The Federal Intelligence Surveillance Court (FISC) in the U.S. holds hearings to approve break-ins for national security reasons. The Bush administration spied and is spying on Americans without the benefit of such hearings.

In the year 2000, the FBI secretly entered the office of Nicodemo Scarfo and installed a keylogger. The FBI was able to capture Scarfo's password and decrypt his PGP-encoded e-mail. The 1971 Watergate goof up was an illegal black-bag operation. In October 1993, Attorney General Janet Reno authorized the FBI to enter the home of Aldritch Ames, a suspected CIA mole. This was after months of electronic and physical surveillance, including searches of his trash [1].

Network wiretap comes with a feature called protocol analysis, which allows it to decode the computer traffic and make sense of it. Network sniffing has a distinct advantage over telephone wiretaps as many networks use shared media, dispensing the need to break into a wiring closet to install the wiretap. This can be done from any network connection and is called promiscuous mode sniffing. However, this shared technology is fast changing to switched technology, which implies that to be effective, the sniffer would be obliged to actively tap the wire [1].

Carnivore is a type of sniffer written by the FBI that scans Internet traffic looking for e-mail messages. It profiles the suspects after analyzing the From: and To: identities of e-mail messages, matching cyber to the real and storing the e-mail messages to the disk. Seemingly Carnivore is a legal instrument, which cannot be installed on a network without a court order and a search warrant for the ISP to comply; however, ISPs have been known to have given sniffing access to the FBI. In the wake of the 9/11 hijacking and air assault, major Internet Service Providers (ISPs) in the U.S. extended total and unqualified cooperation to the federal authorities in the conduct of the investigation of the terrorist attacks [1].

Like NSA, the Carnivore watches the packets go by, then saves a copy of the ones it is interested in. Carnivore was a hush hush affair. The news of its existence broke in July 2000, leading to public furor. The FBI claimed that the Carnivore was designed to conduct efficient wiretaps of e-mail and online communications involving suspected hackers, terrorists, and other criminals [1].

Carnivore is packed in a slim laptop and is described as a tool within a tool that enables the FBI, in cooperation with an Internet Service Provider, to collect counter-intelligence by tapping e-mails or other electronic communications of a targeted user. This is supposed to be done on court orders – something that the Bush administration purposely ignored. Carnivore is used in two ways, like as a content-wiretap and a trap-and-trace, pen-register. Carnivore box consists of a commercial-off-the-shelf (COTS) Windows NT or Windows 2003 box with 256-megabytes of RAM, a Pentium V or higher, 8 to 36 gigabytes of disk space, and a 4G Jaz drive where evidence is something missing. The box has no TCP/IP stack, and therefore, it is hack-proof. A hardware authentication device to control access to the box, and preventing personnel from breaking into the device without leaving telltale signs, is incorporated [1].

Carnivore comes in two pills, the Red one and the Blue one. The former is administered when the ISP claims that it cannot or will not comply with the court order. The Blue Pill is a sophisticated Carnivore program that scans only e-mails where the ISP cooperates for an investigation [1].

Immediately after 9/11, the FBI administered the Red Pill (served EarthLink with a search warrant to gather electronic information relating to national security). With the exception of Earthlink, no one demurred let alone protested when provisions of Foreign Intelligence Surveillance Act (FISA) – which provides guidelines for sensitive investigations by the FBI, CIA, NSA and a handful of other federal organizations, were put into operation. Even Carnivore boxes were installed on servers for the FBI to monitor electronic correspondences of suspected criminals, privacy or no privacy [1].

Earlier, the FBI was using Carnivore in a mode they call Omnivore: capturing all the traffic to and from the specified IP address. DARPA's Genoa Carnivore is now known as DCS 1000. Its effectiveness is yet to be proved, though it is a cutting-edge search engine, a sophisticated information harvesting program, and adopts peer to peer computing methodology [1].

Carnivore can also be used to monitor Internet traffic other than e-mail. Besides e-mail, one common use is to monitor Web traffic: where Web sites are visited, as well as tracking which people might be accessing a particular Web site [1].

There are a number of ways Carnivore and other sniffers can be defeated and Web surfing made anonymous (establishing an SSL connection to proxies), anonymization service and resorting it to remailers, but that would be beyond the scope of this chapter. However, it must be mentioned that cyber tactics is as important a subject as military tactics and it would be wise to teach and learn the tricks of the trade in a formal way [1].

Another equipment of surveillance that merits familiarization with is Real-Time Surveillance System (RTSS). It provides round-the-clock, non-stop, one-window operation with several digital cameras, supporting as many simultaneous camera displays with video recording, synchronized audio recording, motion detection recording and playback with facility for backup. Significantly, it supports live video via dial-up, high bandwidth Internet and LAN. It alarms alerts and has Pan-Tilt-Zoom-Iris-Focus (PTZIF) controls with a remote facility. It also permits networking with several RTSS units, and provides Internet access and surveillance video at 2/3 frames per second. Video watermark technology and passwords make it tamper proof [1].

Today in the e-market, spyware is available that can capture and record every conversation on the Internet Relay Chat (IRC), every transaction and other banking information, passwords, mouse-clicks and keystrokes on the computer, exposing private information to unauthorized public view. Some of the software products have the ability to send this information clandestinely via the e-mail. This spyware is downloadable, worth 80 dollars or so. It can keep a home PC under surveillance from the workplace or vice versa, with salient features of remote keystroke viewing, desktop viewing, application and task management, and open windows management. A good example is that of SpyBuddy, which has features like:

- Internet conversation logging
- Disk activity logging
- Window activity logging
- Clipboard activity logging
- Web site activity monitoring
- Print document logging

- Keystroke monitoring
- Screen shot capturing
- Web-watch keyword alerting
- Remote capture
- Remote system information viewing
- Remote file system navigation
- Remote locking control
- Remote Internet connection monitoring
- Document history viewing
- Mouse freeze control
- Remote Web site launching
- Remote application launching
- Remote shut down and the ability to log chat conversations
- Record all changes made to the hard drive (directories and files), which are created, deleted or renamed.

Fantastic is the world of cyber-spying [1].

Then, there is a variety of anti-spy software (SpyCop, X-Cleaner, Anti-keylogger, NitroU.S. Anti-spy, Evidence Eraser software of the likes of Window washer, Evidence Eliminator Pro and Evidence Terminator). The SpyCop can find:

- Computer monitoring programs used for spying
- Allows renaming any suspect files
- Minimizes software while scanning so that the computer is free to do the other tasks
- Facilitates exploring for hostile spyware by a right click
- Provides a single file-scan function built in complete with browse capability
- Saves results to a text file for future reference
- Prints results directly from the software
- Finds when a spy program was installed
- Checks if a spy program is detectable with database search
- Conducts live updates to a database without re-downloading
- Is unrecognizable to most spy programs
- Has a screensaver, which scans the system when the user is absent [1].

Finally, the purpose of describing the facilities claimed by e-marketed spy and anti-spy software is to impress that in spite of the kind of intelligence and surveillance games that are being played in cyberspace, the vulnerabilities have neither abated, nor cyber security made fail proof and foolproof. Another purpose is to show how technology has completely overshadowed the 007 image of spying and changed its nature from real to virtual (like the Alias and 24 TV shows), and the sweep near to remote. Virus scanners do not detect spyware, and firewalls [6] do not stop their ingress. The one that needs access to the target computer to install spy software is just not true. There are hybrid versions that can be sent just like a virus in e-mail [1].

SUMMARY AND CONCLUSIONS

The U.S. and China take cyber surveillance very seriously. Therefore, let the U.S. get on with it. Finally, that's the only way of becoming a superpower.

REFERENCES

[1] Yashwant Deva, "Cyber Surveillance: Threats and New Technologies," Aakrosh, Forum for Strategic and Security Studies, [Strategic Affairs (Stratmag.com) is an unofficial Defence website, which is not endorsed or recognized by any Government or its institutions. All the material published on this site is in the public domain. The views represented in this site are those of the authors alone.], 2004.

[2] John R. Vacca, Computer Forensics: Computer Crime Scene Investigation, 2nd Edition, Charles River Media, 2005.

[3] Kevin McLaughlin, "RFID Tags May Provide New 'In' For Hackers," CRN, Copyright © 2006 CMP Media LLC, CMP Media LLC, 600 Community Drive, Manhasset, New York 11030, page 57, March 27, 2006.

[4] John R. Vacca, Guide to Wireless Network Security, Springer, 2006.

[5] John R. Vacca, Net Privacy: A Guide to Developing and Implementing an Ironclad ebusiness Privacy Plan, McGraw-Hill, 2001.

[6] John R. Vacca, Firewalls: Jumpstart for Network and Systems Administrators, Digital Press, 2004.