From AFIO's **The Intelligencer**
Journal of U.S. Intelligence Studies
Volume 21 • Number 1 • $15 single copy price **Winter 2014-15**

Association of Former Intelligence Officers
7700 Leesburg Pike Ste 324
Falls Church, Virginia 22043
Web: **www.afio.com**, E-mail: **afio@afio.com**

Guide to the Study of Intelligence

A Guide to Cyber Intelligence

by Douglas R. Price

The Evolution of Cyber Intelligence

Computers came into widespread use in the late 1960s and were used typically for large scientific studies, military planning, and large scale business applications, such as personnel records, payroll, accounting, and data storage. Since such computers often contained information of interest they became an intelligence target. The focus of early intelligence activities was often on recruiting people who had access to the computers of interest and supplying them with tools that would enable access to the information of interest. Computer systems administrators focused on trying to understand their system's vulnerabilities through various systems analyses and penetration testing. Those seeking unauthorized access looked at exploiting these vulnerabilities to bypass the computers' rudimentary protection mechanisms to gain access to other users' data.

As Rand Corporation's Willis Ware noted in 1967:

> *Espionage attempts to obtain military or defense information regularly appear in the news. Computer systems are now widely used in military and defense installations, and deliberate attempts to penetrate such computer systems must be anticipated.*[1]

Ware described a wide range of attacks against computers, ranging from humans (programmers, maintenance staff, etc.) to faulty software to implanted hardware bugs to wiretaps, crosstalk, and unintended radiation of signals from the computer equipment.

In the 1970's, timesharing systems became common and allowed a single computer to be used by several people simultaneously, often from remote locations using modems[2] over telephone lines. As this occurred, cyber efforts broadened to include modem intercepts and techniques for stealing passwords to gain access to the systems.

During the 1980s, as computers started to be connected into networks, access to each computer was granted to a much wider community, often worldwide. This presented new opportunities to intelligence services for clandestinely accessing computers remotely via a network. An early example was the KGB-sponsored German hackers who penetrated several hundred computer systems connected to the US Military's MILNET networks.[3]

Another event that occurred during the 1980s and greatly affected the world of cyber espionage was the introduction of the personal computer (PC). IBM introduced their floppy disk-based PC in 1981, followed by the PC XT in 1983, which came with a hard disk drive. Intel introduced the 32-bit 386 microprocessor in 1985, and a number of vendors cropped up to produce a wide variety of "IBM compatible" personal computer systems. These PCs were incredibly useful for storing information, and came with word processing software that facilitated the production of nicely formatted reports, some of which were of obvious interest to the world's intelligence services.

In the 1980s and 1990s, the PC itself was often the target of an intelligence operation. Typically, an unattended PC in a home, hotel room, or office setting would be physically accessed and the data clandestinely copied. Sometimes, a software bug would be installed (e.g., a keystroke logger) or an electronic transmitter would be planted.[4]

Some intelligence services had the ability to detect from a distance the radio waves emitted by PC electronics and the high voltage cathode ray tube (CRT) computer monitors, which led to the design of TEMPEST shielding and the location of PCs inside specially prepared electromagnetic screen rooms, particularly in embassies and other sensitive work-

1. Willis H. Ware, "Security and privacy in computer systems," AFIPS Spring Joint Computer Conference Proceedings (1967), vol. 30, pp. 287-290, available at *http://www.rand.org/content/ dam/rand/pubs/papers/2005/P3544.pdf.*

2. Acronym for modulator/demodulator, a device for transmitting data over telephone wires by modulating the data into an audio signal to send it and demodulating an audio signal into data to receive it. *dictionary.search.yahoo.com.*

3. This was described by Cliff Stoll in *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*, (New York: Pocket, 1995).

4. A keystroke logger clandestinely records every typed character. See Robert Wallace and H. Keith Melton, *SPYCRAFT: The Secret History of the CIA's Spytechs from Communism to Al-Qaeda*, (New York: Dutton, 2008), and Ronald Kessler, *The Secrets of the FBI*, (New York: Crown Publishing, 2011).

ing spaces.[5] As discussed by Ryan Singel in a *Wired Magazine* article:

> *The principal of the TEMPEST attack is deceptively simple. Any machine that processes information — be it a photocopier, an electric typewriter or a laptop — has parts inside that emit electromagnetic and acoustic energy that radiates out, as if they were tiny radio stations. The waves can even be picked up and amplified by nearby power lines, telephone cables and even water pipes, carrying them even further. A sophisticated attacker can capture the right frequency, analyze the data for patterns and recover the raw information the devices were processing or even the private encryption keys inside the machine.*[6]

In the late 1980s, the first BOTNETs began to appear.[7] BOTNETs spread throughout a network in search of vulnerable computers, which they turn into unwitting agents that execute actions at the direction of the BOTNET controller. Infected computers can be programmed to carry out espionage and covert actions. In fact, many of the methods used in cyber intelligence are derived from the methods used in classical human intelligence (HUMINT) operations. BOTNETs recruit agents (vulnerable computers), communicate with them covertly using a variety of data concealment techniques and dead drops (controlled web servers), and command these agents to do various tasks (disseminate messages, steal or corrupt data, etc.). Today there are armies of these "sleeper agents" embedded as malware[8] on infected computers ready to respond to commands from those who enter instructions from their surreptitiously linked command and control centers.

In the 1990s two other trends emerged: smart phones started incorporating computing capability, and computing devices such as laptops and tablets started incorporating radios for two way communication with cell phone towers and network routers. Smart phones and tablets such as the iPad combine a computer with a cell phone and a wireless internet radio, and are thus subject to a variety of intelligence operations that exploit the devices' computer software, communications, and geospatial characteristics.

As we moved into the 21st century, there was an accelerated trend of using the Internet as a universal connection medium, for which the term "Internet of Things" has been coined. There are already stories appearing about smart refrigerators being hacked to send out spam emails.[9] From a cyber intelligence standpoint, the Internet of Things provides a larger and more diverse set of targets for recruitment.

Tools, Techniques, and Tradecraft

Tools and techniques refer to the basic building blocks of an intelligence capability, such as malicious web servers that install a wide variety of malware on unprotected computer systems. Tradecraft refers to the integrated use of these tools and techniques as part of carefully crafted operations. It is tradecraft that separates a professional intelligence organization from the thousands of hackers that troll the Internet looking for people who naively believe that somebody in Nigeria is going to send them a million dollars. The tradecraft used in cyber intelligence operations parallels the tradecraft used in HUMINT operations, but with the use of automated methods to implement the tradecraft.

The HUMINT activities in Table 1 on the next page are taken from Maloy Krishna Dhar's book *Intelligence Tradecraft*. As can be seen in the table, there are analogous activities in the cyber intelligence realm.[10]

Kim Zetter, writing for *Wired Magazine*, describes one such product called Remote Control System from the Italian firm Hacking Team that controls software that can be clandestinely installed on a variety of smart phones and computers; the total number of these software agents is not mentioned, but they are controlled from 320 command & control servers located in 40 countries worldwide.

> *The new components target Android, iOS, Windows Mobile, and BlackBerry users and are part of Hacking Team's larger suite of tools used for targeting desktop computers and laptops. They allow, for example, for covert collection of emails, text messages, call history and address books, and they can be used to log keystrokes and obtain search history data. They can take screenshots, record audio from the phones to monitor*

5. "TEMPEST: A Signal Problem," *NSA Cryptologic Spectrum*, 1972, available at *http://www.nsa.gov/public_info/_files/cryptologic_spectrum/tempest.pdf*.

6. Ryan Singel, "Declassified NSA Document Reveals the Secret History of TEMPEST," *Wired Magazine*, 29 Apr 2008, available at *http://www.wired.com/threatlevel/2008/04/nsa-releases-se/*.

7. BOTNET is the acronym for robotic network. Timothy B. Lee, "How a grad student trying to build the first botnet brought the Internet to its knees," *The Switch/Washington Post*, 1 Nov 2013, available at *http://www.washingtonpost.com/blogs/the-switch/wp/2013/11/01/how-a-grad-student-trying-to-build-the-first-botnet-brought-the-internet-to-its-knees/*.

8. Short for malicious software.

9. *Science News*, United Press International, "Smart refrigerator hacked to send out spam emails," 17 Jan 2014.

10. Maloy Krishna Dhar, *Intelligence Tradecraft, Secrets of Spy Warfare*, (New Delhi, India: Manas Publications, 2011), and Joel McNamara, *Secrets of Computer Espionage: Tactics and Countermeasures*, (Indianapolis: Wiley; 1st edition, June 20, 2003).

Table 1. Comparing HUMINT and Cyber Intelligence Activities†

HUMINT Activity	Analogous Cyber Intelligence Activity
Spotting and assessing a person	Targeting a computer for malware
Recruiting a source	Spearphishing a computer user
Agent validation (Vetting)	Detection of honeypots
Cover	Useful looking software (with backdoor functions)
Disguise	Benign file names of malware
Sleeper agents	Latent malware on infected computers
Covert communications (COVCOM) to agent	Data hiding for concealment of BOTNET command and control, and data exfiltration
Dead drops	Web servers under BOTNET control
Countersurveillance	Avoiding detection by anti-virus software

† "Spear Phishing" is the practice of sending fraudulent messages to a recipient in order to deceive him into revealing sensitive information such as personal passwords. A "honeypot" is a computer system on the Internet that is expressly set up to attract and trap people who attempt to penetrate other people's computer systems. "Backdoor" refers to a clandestine entry into a computer's software. A "sleeper agent" remains hidden until called to service by his controllers. A "dead drop" is a secret place where spies hide their documents for their controllers to later retrieve.

calls or ambient conversations, hijack the phone's camera to snap pictures or piggyback on the phone's GPS system to monitor the user's location.[11]

Even the computer hardware can be used for espionage purposes. During the 1980s, the Soviets intercepted a number of electronic typewriters headed to the US embassy in Moscow and modified their electronics. An NSA report describes the tampering with these systems.

...found that this implant represented a major Soviet technological improvement over their previous efforts. The bug could be rapidly and easily installed by nontechnical personnel; it resisted detection by conventional methods; and it was wireless and remotely controlled. Search by disassembly and visual inspection, when conducted by any but the best trained technicians, would normally be unproductive... The first goal of the GUNMAN Project, to replace all of the electronic equipment in the U.S. embassy in Moscow with signaturized equipment, was a daunting challenge. Electronic equipment included teletype machines, printers, computers, cryptographic devices, and copiers – in short, almost anything that plugged into a wall socket.[12]

That was 30 years ago. Today's computer systems are filled with integrated circuits (ICs) from all over the world; a typical PC has a dozen or more microprocessors for computing, graphics, keyboard processing, peripheral interfaces, hard disk controllers, DVD and CD ROM controllers, printer controllers, etc. These ICs are relied upon, or "trusted," to perform their expected actions and no more, but there is some concern about having to trust such chips for critical applications. The Defense Advanced Research Projects Agency (DARPA), the Pentagon's R&D wing, has released details about a three-year initiative it calls the Trust in Integrated Circuits program, to address the concern of backdoor functions being built into commercial chips.[13]

Elements of a Cyber Intelligence Program

The Intelligence function is typically described as having a set of functional areas, e.g., collection, covert action, intelligence analysis, and counterintelligence. These areas also apply to Cyber Intelligence.

Cyber Collection

The tools, techniques and tradecraft described above can be applied to a collection operation whose goal is the clandestine acquisition of data from a target computer system. James Gosler, former director of the Clandestine Information Technology Office at CIA, wrote:

Intelligence targets are increasingly using computer networks as the repositories for their secrets. As a result, clandestine photography is rapidly yielding to sophisticated technical operations that exploit these networks. ... Clandestine technical collection no longer requires physical proximity to the target. U.S. information systems can be remotely targeted and their secrets collected and exfiltrated to any part of the world.[14]

Many governments have active cyber espionage

11. Kim Zetter, *Wired Magazine*, 24 Jun 2014, "Researchers Find and Decode the Spy Tools Governments Use to Hijack Phones," available at *http://www.wired.com/2014/06/remote-control-system-phone-surveillance/*.

12. Sharon Maneki, *Learning from the Enemy: The GUNMAN Project*, 2009, (declassified) Center for Cryptologic History, available at *http://www.nsa.gov/public_info/_files/cryptologic_histories/ learning_from_the_enemy.pdf*.

13. Sally Adee, "The Hunt for the Kill Switch," *IEEE Spectrum*, May 2008.

14. James R. Gosler, "The Digital Dimension," in *Transforming U.S. Intelligence*, edited by Jennifer Sims and Burton Gerber, (Washington, DC: Georgetown University Press, 2005).

programs. The Chinese in particular are reported to have a very large and aggressive program of cyber espionage. A recent report by the Mandiant Corporation describes the Chinese cyber espionage organization in detail.[15]

Cyber Covert Action

Cyber intelligence techniques can also be used in support of covert actions, such as disinformation, influence operations, election tampering, sabotage, etc. The Russian adventures in Estonia, Georgia, Ukraine, and elsewhere provide examples of disinformation campaigns being conducted with the help of cyber means, such as hacked web sites.

In 2010, the Iranians discovered that their uranium enrichment program was degraded because the centrifuges in their nuclear facility had malfunctioned. It was discovered that the industrial control system that supervised the centrifuges was corrupted by a specially crafted software package that has come to be known as STUXNET.[16]

Election tampering has long been a focus of covert action by many nations. Researchers have noted that many of the electronic voting machines used to tally votes are vulnerable to tampering. As Joseph Stalin might have said, "It's not who votes that counts, it's who counts the votes." A cyber attack against the voting machines, the systems that read the votes from the machines, the systems used to generate or maintain the software, or a network that interconnects the machines could be used to carry out this type of covert action.[17]

Cyber Intelligence Analysis

A cyber intelligence program must have a strong analytic capability, with multiple levels of analysis. In the initial analysis, closest to the collected data, significant processing and analysis is required to make sense of collected data. The product of collection tends to be raw files, without the overall design. The same is true for collected data packets from a network; extensive analysis is required to put these into a form for higher levels of analysis.

One aspect of cyber intelligence analysis is the study of vulnerabilities. If you're going to study vulnerabilities, whether for purpose of defending against them or using them offensively, you need a way to organize them. The National Geospatial Intelligence Agency has been pioneering the use of Activity Based Intelligence as a means for conducting cyber intelligence analysis. Geospatial refers to developing information about who or what is, was, or will be, where and when. As remarked by Letitia Long, director of NGA:

> *General Keith Alexander, the head of CYBERCOM and the Director of NSA, has challenged NGA to "visualize" cyber. We have accepted that challenge and are using advanced multi-INT fusion and GEOINT techniques – called activity based intelligence – ABI – to answer the General's call and give CYBER COMMAND deeper insights for their strategic, operational, and tactical planning. We are depicting cyber in the physical domain and connecting the "bits and the bytes" with the "bricks and mortar."*[18]

Cyber Counterintelligence

The United States faces a cyber intelligence threat of immense proportions. The defensive (security) community tends to focus on protective features (gates, guards, and guns) and on identifying attackers for prosecution.

Counterintelligence, on the other hand, focuses on understanding the threat: who are the actors, what are their motivations and methods, and how can proven counterintelligence methods counter these threats. In his bookb computer security expert Bruce Schneier presents an excellent methodology for conducting risk assessments using attack trees to model the decision making process of the attacker.[19]

One of the counterintelligence challenges with regard to cyber operations is that of attribution. Often, the details of how an attack occurred can be discovered, but it is difficult to determine who is behind the attack. Given the nature of the Internet, where traffic between points A and B can flow through many nodes located in multiple countries, and the presumed end points can be functioning as relays to repackage, pro-

15. Mandiant Corporation, *APT1: Exposing One of China's Cyber Espionage Units*, 2013, available at *http://intelreport.mandiant.com/*.

16. David Kushner, "The Real Story of STUXNET," *IEEE Spectrum*, March 2013, available at *http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet*.

17. Johns Hopkins University. "Electronic Voting System Is Vulnerable To Tampering: Computer Researchers Find Critical Flaws In Popular Software Produced For US Elections." *ScienceDaily*, 28 July 2003. *www.sciencedaily.com/releases/2003/07/030725081820.htm*.

18. Letitia A. Long, Director, National Geospatial-Intelligence Agency, Prepared Remarks delivered at INSA Leadership Dinner, April 30, 2013, available at *https://www.nga.mil/MediaRoom/SpeechesRemarks/Pages/INSALeadershipDinner.aspx*.

19. Bruce Schneier, *Secrets and Lies: Digital Security in a Networked World*, (Indianapolis: Wiley, 2004).

cess and forward traffic to yet other nodes, it is difficult to state definitively where the commands originated or data ends up.

Weaknesses in tradecraft can be exploited. Reuse of the same methods in multiple operations can be disastrous when breaks into one network can be used to detect and defeat other networks of agents. The technical flaw in the production of one-time pads used by Soviet intelligence in the 1940s was compounded by the fact that these pads were used to report on nearly all Soviet intelligence operations operating in the US at that time. The cryptographic break of this system allowed multiple independent networks of spies to be detected, monitored, and neutralized.[20] One could imagine what would happen if all agents in a given country used the same dead drop, or the same method of communication, or the same disguise, or anything that allows a foreign security service to detect spies via their use of some compromised technique. A similar phenomenon exists in the cyber world. The STUXNET code referred to previously had several variants (e.g., STUXNET, FLAME, DUQU, GAUSS) which have been published by the anti-virus community. If another variant of this code were to show up in the future, it is likely it will be detected quickly.

There is a lot that can be learned from counterintelligence history. During World War II both the allies and the Germans had success turning networks of agents against their masters. The British Double Cross operation and its German counterpart provide examples of how networks of agents can be turned.[21] A similar situation exists in the cyber world, in which botnets of automated agents can be turned by a good CI program to deceive the adversary intelligence service.

The Chinese are mounting a massive economic intelligence operation against the US and others. We could examine history to get some ideas for how to counter this economic espionage. When the Soviets were conducting economic espionage against the US in the 1970s, the Reagan administration responded by using a CI-based covert action program to send a message: We know what you're doing; we don't like it; and we're going to put a stop to it. The FAREWELL case tells how we did this, and it could be applied to the cyber world.[22]

A common mistake by counterintelligence services is to assume that the adversary would operate using the same methods that they use against the adversary. This phenomenon is known as mirroring, viewing the adversary by looking in a mirror at how one's own operations are conducted. In reality, each nation is different in terms of how they conduct intelligence operations due to differences in goals and objectives, available resources, "home turf" advantages, etc. In his book *Tower of Secrets*, Victor Sheymov provides an example of mirroring in which Soviet counterintelligence spent months looking for electronic bugs in its Beijing embassy, only to discover later that the Chinese were using ancient, but effective, methods involving passive acoustic chambers.[23]

Summary

Cyber Intelligence has come a long way since the 1960's and has echoed the evolution of computing and networking technologies. The use of cyber intelligence techniques for clandestine information collection, covert action, and counterintelligence has become commonplace. As the technology world continues to evolve, one can expect the cyber intelligence discipline to keep pace.

Suggested Readings for Instructors

A good overall view of the tools and techniques used in cyber operations can be found in Joel McNamara, *Secrets of Computer Espionage: Tactics and Countermeasures*, (Indianapolis: Wiley Publishing, 2003).

An excellent overview of HUMINT tradecraft is provided in *Spycraft: The Secret History of the CIA's Spytechs, from Communism to Al-Qaeda*, by Robert Wallace and H. Keith Melton, (New York: Plume, 2009).

For an Air Force perspective, in which cyber is viewed in the context of a military conflict, see *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, edited by Jason Healey, published by the Cyber Conflict Studies Association (*http://www.cyberconflict.org/blog/2013/7/23/a-fierce-domain-launches.html*).

For examples of how cyber can be used to support covert operations, see David E. Sanger, *Confront and Conceal, Obama's Secret Wars and Surprising Use of American Power*, (New York: Crown Publishers, 2012).

Doug Price began his career in 1974 as an engineer

20. Nigel West, *Venona: The Greatest Secret of the Cold War*, (London: Trafalgar Square March 2001).

21. Sir John C. Masterman, *The Double Cross System*, (New Haven: Yale University Press, 1972), and Philippe Ganier-Raymond, *Tangled Web: The Shocking and Still Unsolved Story of One of the Greatest Failures of Allied Espionage During World War II*, (New York: Pantheon, 1968).

22. Sergei Kostin and Eric Raynaud, *FAREWELL, The Greatest Spy Story of the Twentieth Century*, (Las Vegas: AmazonCrossing, 2011).

23. Victor Sheymov, *Tower of Secrets, A Real Life Spy Thriller*, (Annapolis: Naval Institute Press, October 1993).

working for NSA's Computer Security Division within its Office of COMSEC Applications. In 1978 he joined System Development Corporation where he performed penetration testing, led red team security studies and designed encryption systems for computer networks. From 1983 until his retirement in 2011, he worked for SPARTA, Inc. developing cyber intelligence tools and techniques. Mr. Price is currently a member of the Board of AFIO.

The Sanctifying of Leakers

Of course, journalists commonly ascribe more noble motives to their sources, and to themselves, than is warranted. Informants leak to reporters for a variety of (sometimes overlapping) motives, including revenge, egotism, self-protection, political ideology, personal or bureaucratic ambition — even, sometimes, altruism.[1] Traditionally, journalists require only that information be verified, not that it be supplied by angels. Still, it is a time-honored tradition to defend the virtue of (your own) sources when they invariably come under attack from those they have implicated in wrongdoing — as Daniel Ellsberg, Chelsea Manning, Edward Snowden, and many other, less famous news informants, have learned. Championing sources as principled whistleblowers is a way reporters attract more of them; calling them out as self-serving snitches would quickly dry up future leaks.

— From "Wallowing Watergate: Historiography, Methodology, and Mythology in Journalism's Celebrated Moment" by Mark Feldstein, 3 Dec 2014, *American Journalism*, 31:4, 550-570.

1. Stephen Hess, *The Government/Press Connection: Press Officers and Their Offices (Washington, DC: Brookings Institution*, 1984), 77–78.

Definitive Guideâ„¢ to Cyber Threat Intelligence. Published by: CyberEdge Group, LLC 1997 Annapolis Exchange Parkway Suite 300 Annapolis, MD 21401 (800) 327-8711 www.cyber-edge.com. I hope you will find cyber threat intelligence a stimulating topic, and this guide a useful resource for your own efforts in the field. John P. Watters Chairman and CEO iSIGHT Partners. Introduction.