By Any Means Possible: How Intelligence Agencies Have Gotten Their Data

Steven M. Bellovin
https://www.cs.columbia.edu/~smb

Abstract

Amidst the many public discussions springing from the Edward Snowden documents, one has been about the perceived change in the NSA's practices: they're now hacking computers instead of tapping wires and listening to radio signals. Looked at narrowly—that is, in terms of only NSA's mission—that may be true. Looked at more broadly, in terms of how intelligence agencies have always behaved, this is no surprise at all. They've long used only two criteria when evaluating a proposed tactic: does it work, and at what cost?

1 Introduction

Everyone knows how governments gather intelligence. There are dashing spies like James Bond (beautiful women optional) and deep cover sleeper agents. Satellites peer into buildings, while brilliant cryptanalysts, in a flash of insight, can crack the strongest "codes". The messages they crack are, of course, intercepted either by stupendous technical feats [27, 20] or by derring-do by the aforementioned dashing and/or beautiful spies.

To say that this concept is false is just as misleading as to say that it is true. Intelligence agencies have always and likely will always acquire information by any means necessary. Their metrics are simple and twofold: Will the scheme work? If it works, is the cost—in people, dollars, and exposure risk—acceptable?

Academics think differently. Confronted with the aforementioned encrypted message, an academic will want to try to attack the algorithm. Success can be defined as differently as full key recovery or a distinguishability attack with a complexity of 2^{230} on a reduced-round version of it. Intelligence agencies just want the plaintext, and getting it because a disgruntled embassy clerk hid it under a bridge is a perfectly acceptable way to succeed. Cryptanalysis may be preferred, but only for its concrete

advantages: it doesn't depend on the foibles and presence of an individual asset who might repent or be detected. The aesthetic aspect, that attacking the algorithm is somehow more "elegant", doesn't enter into the question.

It pays to take a look back through history to see how intelligence has been acquired. The mechanisms used do include spies and beautiful women; they also include satellites, cable taps, strange and wondrous gadgets, and more.

2 Spies and Assets

Spying, of course, is an ancient tradition. One of the oldest recorded instances is given in Joshua 2:1, which was probably composed no later than the 8th century BCE [19] and perhaps two centuries earlier: "Joshua son of Nun secretly sent two spies from Shittim, saying, 'Go, reconnoiter the region of Jericho.' So they set out, and they came to the house of a harlot named Rahab and lodged there." The chapter goes on to relate how she sheltered them and gave them information about the low morale of the city. In return, the spies promised her safety during the forthcoming invasion.

For our purposes, there are three interesting aspects to this tale. First, they consorted with a prostitute, a profession no more respected then than today. Second, they relied on her for information. Third, they made a deal with her: they paid her (with protection from the invading army) for her information and services. These all illustrate practices that are still followed today: dealing with unsavory insiders, relying on them for information, and paying and protecting them. Joshua's spies could have tried to gather the information themselves, but that didn't work out very well earlier in the Bible (Numbers 13). If nothing else, trying to gather information first-hand is risky; indeed, even Joshua's agents were detected (Joshua 2:2): "The king of Jericho was told, 'Some men have come here tonight, Israelites, to spy out the country.'" (To be sure, there is some disagreement on the effectiveness of these spies: Zakovitch thinks they are bumblers [30], while Cardwell of the CIA thinks that they did their jobs very well [5].)

Seducing someone into betraying their country can be done literally, too. "Honey traps"—having someone seduce the target—are used in real life. Kahn [13] tells the story of an agent code-named CYNTHIA, who worked "not for money but for thrills". Her amorous exploits were legion; her conquests included an Italian admiral and a Vichy France press attaché. These "romances" yielded the Italian and French naval codes. The same sort of things go on today. The Soviets were experts at it; the Mossad found that it was easier to turn prostitutes into agents than to ask agents to prostitute themselves [22]. Naturally, it isn't only heterosexual men who are seduction targets; women have been targeted by male agents (this was an East German specialty [15]) and homosexual affairs have often been even better for blackmail.

No one claims that these activities are moral. However, they're perceived as necessary. Most information from human sources—"HUMINT"—is supplied by insiders. This is of necessity; the insiders have the information, and outsiders are too conspicuous. Cases of spies actually penetrating an enemy organization are very rare, though not unknown (see, e.g., the amazing story of Eli Cohen, an Israeli agent who was in line to become Syria's deputy defense minister [12]); far more often, the role of an

agent today, just as in Joshua's time, is to persuade someone else to give them the necessary information. Their role is to persuade the insider, to pay them, and if necessary to exfiltrate them. Yes, there is clever gadgetry, but this is generally for photography, communicating with the actual sources, etc [28].

HUMINT is done this way because it works. That said, there are limits to what spies can accomplish. They can only report what they know, or is contained in documents to which they have access. A well-placed political agent is unlikely to have technical details on weaponry; conversely, a well-placed technician will have little idea what political decisions are being made. Beyond that, spying is risky, both personally and politically. Agents have a finite lifetime before they fall under suspicion or burn out; when these things happen, exfiltrating them becomes crucial. This is partly because it's good practice—few prospective spies will want to work for a country that abandons its assets—but also because captured spies carry a cost, in embarrassment and in what they can be forced to reveal about other operations.

3 Intercepting Communications

To cope with some of the limitations of human agents, intelligence agencies have long resorted to other means. One has been interception communications, and thus gaining an insight into the other side's actual operational plans. Kahn wrote, of an incident during World War I, that [13]:

> It was, in fact, nothing less than a full roundup of the situation as Samsonov saw it, together with the most detailed and explicit moves to be followed by his army. It gave the Germans a knowledge of enemy intentions unprecedented in the whole of military history. It was like reading the mind of a chess opponent, like playing blind man's bluff without the blindfold. It was almost impossible to lose.

Militaries were not slow to realize this. Communications interceptions are about as old as the use of communications for military purposes; not surprisingly, so are defenses. The ancient Greeks had their skytales; the Romans had the Caesar cipher [13]. During the Renaissance, diplomats communicated via sealed, encrypted letters; kings therefore set up "Black Chambers" that would open, copy, decrypt, and reseal these messages. When, during the US Civil War, the telegraph became important, interception of telegrams followed quickly. Jeb Stuart, a Confederate general, "actually had his own personal wiretapper travel along with him in the field" [8].

As technology improved, so did both attacks and defenses. Intelligence threats to telegraph cables became a major driver in British communications strategy. The ability to send messages via an "all red route"—that is, solely via stations located in British possessions, which were colored red in the maps of the time—became a major driver in selecting paths for new telegraph links [14]. Conversely, they were not slow to appreciate the intelligence capabilities they had acquired by virtue of being the hub of the world's telegraph network; indeed, the Official Secrets Act of 1920 contained a provision that effectively required copies of all international telegrams transiting the United Kingdom to be turned over to Naval Intelligence.

Radio made interception easier; naturally, the world's spy agencies built elaborate interception facilities. Defenders countered with encryption; they, too, resorted to technology. Hand encryption systems were too slow for volumes of traffic and were insecure to boot, so mechanized systems were developed: Vernam's one-time tape Teletype, Scherbius's Enigma, and more. Cryptanalysts countered with automation of their own, both off-the-shelf punch card machines and custom devices [13, 6, 26]. The culmination of this trend was computerization of cryptanalysis. The first such machine, the Colossus, was also the first programmable electronic computer; it was built at Bletchley Park to crack the German Lorenz ("Tunny") cipher [10]. The trend has continued. One of the customers for IBM's Project Stretch, an effort to produce a computer 100 times faster than the IBM 704 [4], was the NSA. The resulting computer, the IBM 7030, even had a special cryptanalytic add-on called Harvest, described in the open literature as a "Nonarithmetical System Extension". The NSA is still building massive computing complexes [2].

More interception elaborate techniques have been used as well. Spy subs have tapped undersea cables [27]. Hidden microphones have picked up the sound of rotor wheels being set [29]. Specialized ships, planes, and satellites have all been used to collect radio signals.

Communications interception can work well, and if done by technical means is often undetectable. If the activities are detected or disclosed, there can be considerable public outrage—witness the uproars about ECHELON and the Snowden revelations—but intelligence agencies often shrug off such problems. There are, however, two obstacles: the increasing volume of communications means that there's a vast amount of data to collect and sift through in search of the really interesting material, which in turn translates to vastly increased cost; second, the growth in strong encryption means that the actual yield is less. To be sure, the growth in machine-readable data—it's easier to process structured text than voice—and the amazing haul in metadata have at least partially compensated, but there is constant concern about "going dark".

4 Overhead Surveillance

Spying moved overhead as soon as it was technically possible. In the US Civil War, balloons were use from the beginning for "reconnoissance" [sic], and was used in Europe even earlier [3]: "The importance of gaining such a height for observation can be appreciated by all readers of military annals" [18].

Naturally, progress did not stop with balloons; reconnaissance aircraft played major roles during both world wars. In fact, aerial reconnaissance was so pervasive during World War II that the British used "accidental" sightings of German ships to disguise the real way they knew their location: cryptanalysis. Aerial reconnaissance was so common that it need not be concealed.

Two of the most famous planes in history, the U-2 and the SR-71, were spy planes. Built at Lockheed's legendary Skunk Works [23], one of their primary missions was observing the Soviet Union's nuclear capabilities [24]. The U-2 became vulnerable to improved Soviet air defenses, of course, but a replacement was ready in time: the first spy satellites were ready.

These early satellites were a technological tour de force: for lack of suitably compact television cameras, they periodically ejected film canisters which were caught in midair by specially equipped airplanes. This sounds like an amazing spur-of-the-moment response to an intelligence crisis, but it wasn't; the US had been planning for orbital spying since at least 1950 [16]: a satellite would be a "novel and unconventional instrument of reconnaissance." In fact, one motivation for launching scientific satellites during the International Geophysical Year was to provide legal precedent for satellites overflying other countries [16]; IGY was under UN auspices.

Modern spy satellites are much more sophisticated, of course. Indeed, the mirror technology for the Hubble Space Telescope was the same used for spy satellites [9]. In addition, there are many specialized types: ELINT (electronic intelligence), radar ocean reconnaissance, missile warning, communications interception, and more [7].

Overhead reconnaissance works, but there are limits. Cameras can't see inside buildings. Clever adversaries can time their activities to evade satellites; there have been claims that India did exactly that to hide preparations for its 1998 nuclear tests [1, 25, 24]. Airplanes have less predictable coverage patterns, but of course they can be shot down. It will be interesting to see how drone-based platforms fare.

5 Enter the Computer

Legend has it that when Willy Sutton, the bank robber, was asked why he robbed banks, he replied, "That's where the money is." Intelligence agencies follow a similar philosophy: they'll go where the data is. Today, much of the world's information is created on, transmitted from, and received by computers. This alone would make computers a interesting target. In addition, the explosive growth of strong cryptography has rendered traditional communications intercepts much less useful. The solution—capturing the data before encryption or after decryption—is obvious, *if* it can be done. It can. Furthermore, the techniques necessary, such as hacking software, are useful for other forms of collection. For example, modern phone switches are nothing but computers with odd peripherals attached; these computers can be hacked, too.

At this point, we know little of how computer espionage is done, by whom, or its scope. There have been a few published reports, mostly focusing on economic espionage, e.g., [17]. Occasional failed operations, such as an operation that penetrated a mobile phone switch in Greece [21], give some hint of what can be done. In other cases, government-grade spyware has been discovered. Flame, for example, used a previously unknown cryptanalytic attack on the MD5 hash function [11]. In other words, we know neither the details nor the scope, but we've seen enough to know what's going on: as always, spying has followed technology, and now has moved into cyberspace. That may be upsetting, but it can't be considered a surprise.

References

[1] AP. “CIA Searching for Answers Behind its India-Nuclear Failure”. In: *Associated Press* (May 16, 1998). URL: http://www.fas.org/irp/news/1998/05/may16_cia.html.

[2] James Bamford. “The NSA Is Building the Country’s Biggest Spy Center (Watch What You Say)”. In: *Wired: Threat Level* (Mar. 15, 2012). URL: http://www.wired.com/2012/03/ff_nsadatacenter/.

[3] Eugene B. Block. *Above the Civil War; the story of Thaddeus Lowe, balloonist, inventor, railway builder*. Berkeley, CA: Howell-North Books.

[4] Werner Buchholz, ed. *Planning a Computer System: Project Stretch*. New York: McGraw-Hill, 1962. URL: http://archive.computerhistory.org/resources/text/IBM/Stretch/pdfs/Buchholz_102636426.pdf.

[5] John M. Cardwell. “A Bible Lesson on Spying”. In: *Studies in Intelligence* (Winter 1978). URL: http://southerncrossreview.org/44/cia-bible.htm.

[6] Elliot Carlson. *Joe Rochefort’s War: The Odyssey of the Codebreaker Who Outwitted Yamamoto at Midway*. Annapolis, MD: Naval Institute Press, 2011.

[7] Central Intelligence Agency. *Soviet Military Capabilities and Intentions in Space*. National Intelligence Estimate 11-1-80. 1980. URL: http://www.foia.cia.gov/sites/default/files/document_conversions/89801/DOC_0000284010.pdf.

[8] Samuel Dash, Richard F. Schwartz, and Robert E. Knowlton. *The Eavesdroppers*. New Brunswick, NJ: Rutgers University Press, 1959.

[9] Andrew J. Dunar and Stephen P. Waring. *Power to Explore: A History of Marshall Space Flight Center 1960–1990*. The NASA History Series. Washington, DC: National Aeronautics and Space Administration, 1999.

[10] Jack Good, Donald Michie, and Geoffrey Timms. *General Report on Tunny: With Emphasis on Statistical Methods*. HW 25/4 and 25/5. UK Public Record Office, 1945. URL: http://www.alanturing.net/turing_archive/archive/index/tunnyreportindex.html.

[11] Dan Goodin. “Crypto Breakthrough Shows Flame Was Designed by World-Class Scientists”. In: *Ars Technica* (June 2012). URL: http://arstechnica.com/security/2012/06/flame-crypto-breakthrough/.

[12] Jacob Javits. “Superspy in an unholy war”. In: *Life* 71.2 (July 9, 1971).

[13] David Kahn. *The Codebreakers*. New York: Macmillan, 1967.

[14] Paul M Kennedy. “Imperial cable communications and strategy, 1870-1914”. In: *English Historical Review* 86.341 (Oct. 1971), pp. 728–752. URL: http://www.jstor.org/discover/10.2307/563928?uid=2&uid=4&sid=21103708309471.

[15] Phillip Knightley. “The History of the Honey Trap”. In: *Foreign Policy* (Mar. 12, 2010). URL: http://www.foreignpolicy.com/articles/2010/03/12/the_history_of_the_honey_trap.

[16] Walter A. McDougall. *The Heavens and the Earth: A Political History of the Space Age*. New York: Basic Books, 1985. URL: http://quod.lib.umich.edu/cgi/t/text/text-idx?c=acls;idno=heb00674.

[17] Office of the National Counterintelligence Executive. *Foreign Spies Steaing US Economic Secrets in Cyberspace*. Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009–2011. Oct. 2011. URL: http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.

[18] Ed. Pietsch. “The War Balloon at General M’Dowell’s Head-Quarters Preparing for a Reconnoissance”. In: *Harper’s Weekly* (Oct. 26, 1861), p. 687.

[19] Frank H. Polak. “The Oral and the Written: Syntax, Stylistics, and the Development of Biblical Prose Narrative”. In: *Journal of the Ancient Near Eastern Society* 26 (1998), pp. 59–105. URL: http://www.jtsa.edu/Documents/pagedocs/JANES/1998%2026/Polak26.pdf.

[20] Norman C. Polmar and Michael White. *Project Azorian: The CIA and the Raising of the K-129*. Annapolis, MD: Naval Institute Press, 2010.

[21] Vassilis Prevelakis and Diomidis Spinellis. “The Athens Affair”. In: *IEEE Spectrum* 44.7 (July 2007), pp. 26–33. URL: http://spectrum.ieee.org/telecom/security/the-athens-affair/0.

[22] Dan Raviv and Yossi Melman. *Spies Against Armageddon: Inside Israel’s Secret Wars*. New York: Sea Cliff, 2012.

[23] Ben R. Rich and Leo Janos. *Skunk Works: A Personal Memoir of my Years at Lockheed*. Boston: Little, Brown, 1994.

[24] Jeffrey T. Richelson. *Spying on the Bomb : American Nuclear Intelligence from Nazi Germany to Iran and North Korea*. New York: Norton, 2006.

[25] James Risen, Steven Lee Myers, and Tim Weiner. “U.S. May Have Helped India Hide Its Nuclear Activity”. In: *New York Times* (May 25, 1998). URL: http://www.nytimes.com/1998/05/25/world/us-may-have-helped-india-hide-its-nuclear-activity.html.

[26] Frank B. Rowlett. *The Story of MAGIC: Memoirs of an American Cryptologic Pioneer*. Laguna Hills, CA: Aegean Park Press, 1998.

[27] Sherry Sontag and Christopher Drew. *Blind Man’s Bluff: The Untold Story of American Submarine Espionage*. New York: Public Affairs, 1998.

[28] Robert Wallace, H. Keith Melton, and Henry R. Schlesinger. *Spycraft: The Secret History of the CIA’s Spytechs, from Communism to Al-Qaeda*. New York: Dutton, 2008.

[29] Peter Wright. *Spycatcher: The Candid Autobiography of a Senior Intelligence Officer*. Viking, 1987.

[30] Yair Zakovitch. “Humor and Theology, or the Successful Failure of the Israelite Intelligence (Josh. 2): A Literary-Folklorist Approach’”. In: *Text and tradition : the Hebrew Bible and folklore*. Ed. by Susan Niditch. 1990, pp. 75–98.