4

National Security

In discussions of cryptographic policy, "national security" is usually shorthand for *communications intelligence*—spying on foreign communications. It is taken for granted that the United States depends on breaking foreign codes for much of its intelligence and that any decline in the success of this activity will make the country less secure. Intelligence, however, is only one of cryptography's roles in national security.

The Concept of National Security

The notion of national security is a relative newcomer to American political iconography. Although the term dates to the early post-World War II era, it does not appear in *Webster's Third International Dictionary*, which was published in 1961 and which sought to capture an up-to-date picture of American English.

The essence of national security is, of course, the protection of the country against attack by foreign military forces. The term is broader than this, but not so broad as to encompass all of the national interest. Its focus is protection of the country, and in particular its government, against threats that are characteristically but not invariably foreign.

National security includes the following:

- Maintenance of military forces adequate to deter attacks on the United States, repel invaders, control domestic unrest, and undertake other military actions that may be in the national interest.
- Provision of intelligence on the capabilities and intentions of all powers, both friendly and hostile, sufficient to inform foreign pol-

icy and military action. Such powers are understood to be primarily, but not entirely, national states. They may, in addition, include organizations representing landless peoples, revolutionary movements, terrorist groups, organized crime, trans-national political movements, and multi-national corporations.

- Denying to foreign powers intelligence about the United States that would interfere with American diplomatic, military, or trade objectives.
- Enforcement of certain laws, in particular those governing espionage, terrorism, the integrity of the national-security community itself, and the movements of people and material across borders.
- Maintenance of an industrial base, a resource base, and an infrastructure adequate to support essential government activities, including military forces, intelligence, and relevant aspects of law enforcement.

The set of issues that define the national security is naturally neither free from debate nor immune to change. In the late 1960s and the 1970s, the idea that drug trafficking should be seen as a threat to the national security and approached with military resources and tactics gained substantial ground.[1] Since the end of the Cold War, a quite different constituency has argued for the inclusion of broader economic issues, such as education and competitiveness in the world marketplace.[2]

From the viewpoint of communications security—and its all-important component, cryptography[3]—the relevance of the second and third points —intelligence and security against foreign intelligence—is most apparent. We will examine these first and in more detail, but issues of infrastructure, law enforcement, and offensive capability will also be considered.

The Spectrum of Intelligence

When we speak of intelligence, we will usually mean national intelligence —information obtained by national governmental organizations. The intelligence activities of governments, however, have much in common with those of other organizations. Scholars, reporters, political parties, businesses, criminals, and police all practice intelligence in one form or another. The intelligence-gathering activities of nations are generally more ambitious and include things not accessible to organizations without state power (for example, launching spy satellites), but the similarities outweigh the differences.

The most familiar form of intelligence—so familiar that it is usually not recognized as intelligence—is *open-source intelligence*: information obtained from sources that are not attempting to conceal it. Open-source intelligence is almost the only form of intelligence practiced by scholars, reporters, and business people, but it also plays a major role in national intelligence. In the national case, typical open sources are newspapers, radio broadcasts,[4] foreign government publications, propaganda, maps, and phone books. In industrial intelligence, advertisements and product literature are major sources.

Older open sources have now been joined by the Internet and the World Wide Web. Browsing the Web is practicing open-source intelligence. Google and more specialized search engines give their users access to information on an unprecedented scale.

Operations intelligence is information obtained by observing and recording a target's visible actions and inferring actions that are not visible. Although it is hardly limited to military affairs, a typical example of operations intelligence in a military context was widely touted during the 1991 Gulf War: a pizza parlor near the Pentagon told newsmen that it could always tell when something was about to happen because large numbers of people stayed late at the Pentagon and ordered pizza in the middle of the night.[5]

What most people think of when they think of "spying" is called *human intelligence* (HUMINT), which runs the gamut from interviewing travelers[6] to infiltrating illegal agents and sometimes extends to breaking and entering. In the most basic form of human intelligence, intelligence officers from one country, traveling under diplomatic or journalistic or commercial cover, recruit an agent who has access to secret information. The agent then passes information to the foreign handlers, usually either for ideological reasons or in exchange for money.

In the twentieth century, open-source intelligence, operations intelligence, and human intelligence were joined by a host of new methods having only the barest antecedents.[7] Indeed, David Kahn, cryptology's foremost historian, argues that modern intelligence was created by signals intelligence (Kahn 2006). Generals were unwilling to commit their resources and risk their troops on the words of spies. Only when radio interception gave them access to their opponents communication did they have intelligence they were prepared to believe.

The growth of technology intensive intelligence originated in the use of new technologies to gather intelligence about societies that exercise tight control over the information they release to the outside world and over the movement of people across and within their borders. Their success has pushed back the frontiers of national sovereignty; by limiting the degree to which nations can keep their military preparations secret from each other, it has also become a fundamental stabilizing influence on international relations. For the United States, surprised once by the Japanese at Pearl Harbor and again by al-Qaeda on 9/11, intelligence has become a national obsession.

The techniques of intelligence gathering have also been guided by adaptation to political reality. Throughout the twentieth century, improvements in communication and increases in interdependence have produced the "shrinking of the world" that has changed so much of modern life. This has increased peer pressure among nations, giving rise to the World Court, the United Nations, and other international institutions. In this environment, nations have become more concerned than ever with appearance.

Spying exists, and has perhaps always existed, in a sort of limbo. "Everyone" knows that "everyone" does it, yet it remains frowned upon, hidden, and, under the laws of the nation being spied on, illegal. Most if not all nations use their embassies and consular facilities forintelligence gathering. Some of the activities are aboveboard. Ambassadors, trade representatives, and military attachés all report on both their meetings with representatives of the host country and their observations of life, politics, industry, and military activity. Others are not. Embassy personnel often recruit spies from among the local population or undertake more technical forms of information gathering from the legally protected premises of the embassy (Frost 1994).

Often a host country is aware of the clandestine intelligence activities of foreign diplomatic and consular personnel but finds itself unable to interfere for fear of retaliation against its own diplomats. When an espionage case becomes public, the host country usually feels obliged to put on a show of public indignation, and a scandal ensues. Such was the case when Soviet Colonel Oleg Penkofsky was caught spying for the West in the 1960s, and more recently when CIA officer Aldrich Ames was caught spying for Russia. The embarrassment is most acute when the countries involved are supposed to be friends, as happened in the case of Jonathan Pollard, an American naval intelligence officer found to be spying for Israel. A desire to avoid embarrassments of this sort is one motivation for the development of a variety of new forms of intelligence that do not intrude on the territory of the target country.[8]

Another outgrowth of the "shrinking" is the relationship between the tactical and the strategic. The time-honored practice of climbing a hill to get a look at an opposing army—which, in the past, was of little use except during battle—has evolved into a new field of strategic reconnaissance.

No aspect of modern intelligence is more impressive or more important than *photographic intelligence* (PHOTINT): information from photographs at frequencies both in and out of the human visual range. Although photography dates from the nineteenth century, it did not become a distinctive tool of intelligence until aircraft and later spacecraft gave cameras secure platforms from which to operate—platforms that could observe an opponent's territory from a safe distance.

Today, the most important intelligence photographs are those taken from orbiting satellites. Paradoxically, despite the fact that photo-reconnaissance aircraft fly much closer to their targets than satellites (10–20 miles as opposed to several hundred), the larger cameras carried by satellites produce far more detailed pictures. Images of a Russian shipyard taken by an American KH-11 spy satellite appear to be from a distance of 500 feet rather than the actual 500 miles (Burrows 1987, pp. 166n–166o; Richelson 1990, p. 186).

Photographic intelligence provides high-resolution images of the Earth's surface but is impeded by clouds, sandstorms, and vegetation. The passive form is therefore complemented by the use of radar-imaging satellites, such as the American Lacrosse, which produce lower-resolution images but are unaffected by night and fog and can penetrate trees and even buildings. Orbital lasers open yet other possibilities (AWST 1997b).

Besides cameras and radar, modern intelligence employs a broad range of sensors for *measurement and signatures intelligence* (MASINT), which seeks to characterize objects or events by their observable characteristics and to detect or analyze them by combining information from various sensors. In the late 1940s, the United States began collecting atmospheric samples and testing them for radioactive isotopes in an attempt to discover nuclear tests. It was this technique that made the US aware of the Soviet Union's successful test of a nuclear weapon before it was announced. At about the same time an Air Force activity named *Project Mogul* sought to listen for the sounds of nuclear explosions propagating along the boundaries between layers of the atmosphere.[9]

For decades, the *Sound Surveillance Underwater System* (*SOSUS*) has tracked the movements of submarines and other ships by means of arrays of microphones lying on the ocean floor. In the 1960s, a family of satellites called Vela-Hotel were put in orbit to watch the earth for nuclear explosions. These satellites exemplify the *signatures* aspect of intelligence, distinguishing nuclear events from other phenomena such as lightning flashes or meteor impacts by characteristics more subtle than the brightness of the flash.[10] More recent satellites called simply Defense Support Program satellites also watch for the infrared signatures that characterize the exhaust plumes of rising ballistic missiles. Satellites were only one part of the wider Vela program for detecting nuclear explosions. Another important element was seismographic. An array of seismometers called *NORway Seismic ARray* (*NORSAR*) was placed at a location geologically coupled to the area in which the Soviets conducted their nuclear tests. Seismic measurements served to verify compliance with a treaty limiting the yields of underground nuclear explosions.

Measurement and signatures intelligence can be viewed as a refined form of operations intelligence. It seeks out one or more subtle but unavoidable consequences of an event and infers the occurrence and character of that event from the observed phenomena. Its efficacy depends not only on the sensors but on the computing required to draw useful inferences from the data they produce.

Another aspect of modern intelligence that leans heavily on inference may be called *technical intelligence*. As the term suggests, this is the study of an opponent's technology, but the emphasis in this case is on inferences drawn by simulating or duplicating technologies whose existence has been inferred from observations or from information provided by human sources. The British Office of Scientific intelligence made extensive use of such methods during World War II to improve its understanding of developing German weaponry. Accounts of its work convey a novel perspective in which the reports of human agents were essentially regarded as rumors to be confirmed or refuted by technical means (Jones 1978; Johnson 1978).

The various means of gathering intelligence are far from independent. This is true both in the sense that the boundaries are not sharp (it is sometimes difficult to pigeonhole something as photographic intelligence rather than imaging intelligence) and in the sense that frequently information obtained by one technique may be useful or even indispensable in acquiring information by another technique or in interpreting the information acquired by another technique.[11]

Signals Intelligence and Communications Intelligence

We have surveyed a variety of forms of intelligence in an attempt to convey the breadth of modern intelligence work. No one intelligence method exists in a vacuum, and the intelligence analyst draws on information from a wide variety of sources. It is within this context that we now turn to the form of intelligence with which we are most concerned.

Communications intelligence (COMINT) is the practice of extracting information from an opponent's communications. Although, as we shall see, communications intelligence is quite broad, it is embedded within a yet broader category. *Signals Intelligence* (SIGINT) is the information obtained by analyzing signals emitted by a target. When signals intelligence is distinguished from communications intelligence, the broader category includes such electromagnetic phenomena as radar signals, which are not intended to convey information but rather to locate physical objects and measure their movements. The study of radar signals is at the heart of electronic warfare and is prerequisite to all efforts either to jam radars or to evade them by stealth.[12] The areas of signals intelligence other than communications intelligence are collectively called *electronic intelligence* (ELINT) and include *radar intelligence* (RADINT), *telemetry intelligence* (TELINT), and *emissions intelligence* (EMINT).

Although normally categorized as electronic intelligence, some aspects of emissions intelligence can be better regarded as communications intelligence. These include processing ciphertext to extract plaintext signals accidentally encoded "piggyback" and listening to the sounds of electromechanical cryptoequipment as an aid to cryptanalysis (Martin 1980, pp. 74–75; Wright 1987, p. 84; Agee 1975, pp. 474–476). Another aid to communications intelligence is *emitter identification*, the technique of distinguishing individual radio transmitters by minor variations in behavior too small to be eliminated by ordinary quality-control techniques.

One of the most disquieting techniques of emissions intelligence is Rafter, a technique for monitoring the behavior of radio receivers.[13] It is not surprising that it should be possible to exploit the signal of a radio transmitter. That a receiver should reveal the frequency it is listening to is both surprising and frightening. It can be used, for example, to determine who is listening to banned foreign radio broadcasts.

Despite the elaborate taxonomy, the distinctions are not always clear. Telemetry intelligence, for example, is the study of communications between moving platforms (usually aircraft, rockets, or satellites) and their controlling stations. Test firings of ballistic missiles are monitored via radio transmissions from the missile being tested, and interception of these signals permits an opponent to learn almost as much from the test as do the people conducting it.[14] Similarly, communication satellites, spy satellites, and others are controlled from the ground, and interception of the control channel can reveal information about a satellite's attitude, fuel supply, and activities.[15] It is clear that these examples of telemetry intelligence, though commonly classified as signals intelligence, are as much examples of communications intelligence.

In short, although the term SIGINT is sometimes used to distinguish interception of non-communications signals from communications signals, it is also used to encompass both activities. Communications intelligence so dominates signals intelligence that the term "SIGINT" is often used when the narrower term "COMINT" would do.

With the possible exception of human intelligence, communications intelligence exhibits unparalleled breadth and flexibility. Observation of the gross characteristics (often merely the occurrence) of messages can be used to monitor military, diplomatic, commercial, or criminal activity or to detect relationships between persons, organizations, or events that have, to public appearances, no connection.[16] On the other hand, the analysis of carefully selected messages can sometimes reveal the intentions of military or political leaders even more accurately than information obtained by recruiting members of their staffs.[17]

Because it relies primarily on radio reception, with only occasional recourse to transmission or physical taps, communications intelligence rarely results in diplomatic incidents; indeed, rarely is the target aware of being monitored.[18]

Taxonomy of COMINT

Cryptography is often considered, particularly by those primarily concerned with security, to be the only serious barrier to communications intelligence. Histories of the field have generally fostered this impression by painting a picture of war between codemakers and codebreakers. In practice, spying on communications is a multi-stage activity in which each stage plays an essential role. It is entirely possible that the cryptanalysis of a message, once the message has been identified and captured, may be less difficult than acquiring and filtering the traffic to locate it. On balance, the greatest problem in communications intelligence—as in most efforts to learn things—is sorting out the information you are after from the information you are not.

The *sine qua non* of communications intelligence is acquisition of signals. Without communications in the form of radio waves, electrical currents in wires, written materials, or copied disks and tapes, there can be no work for cryptographic or intelligence analysts. The interception of communications presents both a strategic and a tactical aspect.

Strategically, it is crucial to learn as much as one can about an opponent's communications infrastructure. The first step is to come up with the most precise possible description of the target—what the military call the *order of battle*. If the target is a country, it may have millions of residents who in turn make millions of phone calls every day. Most of these calls are not of interest; the people who make them do not work for the government or in critical industries and say little of intelligence value. Describing the target is one of the many areas where *collateral intelligence*—information from sources other than covert interception of communications—plays a vital role. Most of the information about a country and its government can be learned from open sources, such as phone books, newspapers, histories, and government manuals. Some, however, will come from covert sources such as spies, and some will come from communications intelligence itself.

Once the targets have been precisely identified, it is necessary to discover how they communicate with one another. Are their communications carried by high-frequency (HF) radio, by satellite, or by microwave? How accessible the communications are and how they can be acquired is a function of the means chosen. High-frequency radio and satellite transmissions are the most accessible. At the time of World War II, most radio communication and thus most of what was intercepted was HF. Such signals bounce back and forth between the ionosphere and the ground and can travel thousands of miles. This property makes intercontinental radio communication possible; at the same time, it makes it essentially impossible to keep HF signals out of the hands of opponents. Today a large fraction of radio communication is carried by satellite. Satellite downlinks typically have "footprints" thousands of miles across that spread over more than one country.[19] Terrestrial microwave communications are significantly harder to intercept. They travel between towers a few miles or tens of miles apart. Intercept facilities on the ground must generally be located within a few tens of miles of the microwave path and often require facilities in the target country.[20] Terrestrial microwave is nonetheless vulnerable to interception by an astounding, if expensive technique: satellites on the microwave path beyond the receiving antenna. The satellite is in synchronous to orbit remain in the same relative position to its microwave targets. It is placed not over the target country but about a quarter of the way around the Earth from the target (Campbell 1999).

As with the organizational structure, a target's communication practices can often be derived from open sources. Since national and international organizations cooperate in allocating the radio spectrum, it is easier to identify the frequencies used for military, police, or air traffic

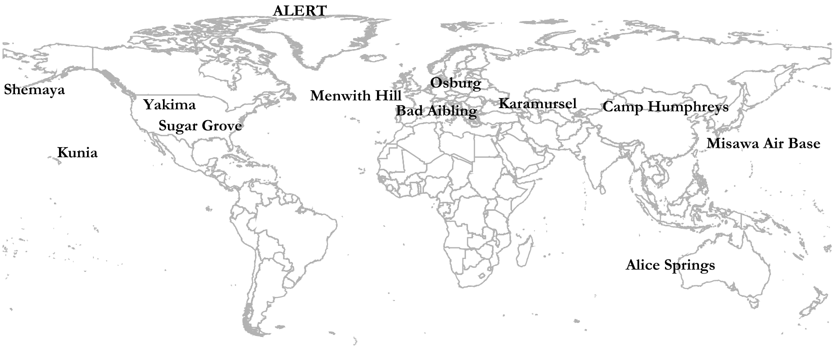

Figure 4.1
NSA installations around the world. (Illustration by Roland Silver.)

control communications by consulting regulations and standards than by direct spectrum monitoring.

The output of the strategic or *targeting* phase of communications intelligence is a map of the opponent's communications, which will guide the selection of locations, frequencies, and times of day at which monitoring is conducted. Interception can also be conducted from many sorts of platforms: ground stations, aircraft, ships, embassies, covert locations, and orbiting satellites.

The United States has several major intercept facilities within its borders and a host of others abroad (figure 4.1). Despite attempts to keep these locations secret, many, including Menwith Hill in Britain, Alice Springs in Australia, Alert in Canada, Osburg in Germany, Misawa in Japan, and Shemaya in the Aleutian Islands have been in the news at one time or another (Bamford 1982; Shane and Bowman 1995).

The Soviet Union made extensive use of small ships as collection platforms. Usually operating under very thin cover as fishing trawlers, these boats carried large antennas and were thought to be making their biggest catch in the electromagnetic spectrum. The United States has been less successful with this approach. In the 1960s it commissioned two ships described as research vessels, the *Liberty* and the *Pueblo*, for intercept duty. The *Liberty* was attacked by the Israelis, for no publicly apparent reason, while supposedly intercepting Arab communications in the Eastern Mediterranean during the Six Day War of 1967.[21] A year later, the *Pueblo* was captured by the North Koreans. It turned out to have been carrying many TOP SECRET documents for which it had no apparent need, and most of these fell to its captors. As quietly as it had begun, the United States ceased using small ships as collection platforms.

Airborne collection, by comparison, has been an important component of US COMINT for decades. Boeing 707s, under the military designation RC-135, are equipped with antennas and signal-processing equipment. These aircraft can loiter off foreign coasts for hours at a time. Flying at altitudes of 30,000 feet or higher, they can pick up radio transmissions from well inland.

The use of embassies to do intercept work exemplifies the twilight-zone character of intelligence. Despite widespread "knowledge" that many embassies are engaging in intelligence collection, such activity is a breach of diplomatic etiquette that could result in diplomats' being asked to leave the host country if discovered. All the equipment used must therefore be smuggled in or constructed on the spot and must be made from components small enough to fit inconspicuously in the "diplomatic bag" —a troublesome limitation on the sizes of antennas. Politics and public relations aside, if an embassy is not suspected of interception, it is likely to be more successful. Mike Frost, a Canadian intelligence officer who spent most of his career intercepting host-country communications from Canadian embassies, reported that the Chinese put up a building to block radio reception at the US embassy in Beijing but failed to protect themselves against the Canadian embassy because they did not realize that it too was engaged in interception (Frost 1994).

Interception can also be conducted from covert locations that do not enjoy the legal protection of diplomatic immunity. Britain operated a covert direction-finding facility in neutral Norway during World War I (Wright 1987, p. 9). In the early 1950s, the CIA established a group known as "Staff D" to carry out interception from covert locations.

One of the most ambitious undertakings in communications intelligence has been the development of intercept satellites, which did not arrive on the scene till roughly a decade after their camera-carrying cousins. Low-altitude satellites are not well suited to intercept work. They are relatively close to the transmitter, which is good, but they are moving quickly relative to the Earth, which is not. No sooner have they acquired a signal than they move on and lose it again, because the source has passed below the horizon. The comparison with communications satellites is interesting. The mainstay of satellite-mediated communications has been satellites in synchronous orbits, 22,500 miles up. Only recently have communications satellites been placed in low orbits. Tens of satellites are required so that as soon as one moves out of range of a transmitter on the ground, another comes close enough to take over. Systems of this kind have the advantage that the satellites and the transmitters are cooperating. A system in which the satellites were attempting continuous coverage of uncooperative targets would be far more complex.

Because they are in very high orbits, intercept satellites must carry antennas tens or hundreds of feet across. It is difficult to make an antenna of this size light enough to be lifted into synchronous orbit. In addition, the antenna must be launched in a folded configuration, which adds complexity and detracts from reliability. In sum, communications intercept satellites are more complex and expensive than other types.

Because of its huge size and the low population density of much of its territory, the Soviet Union made more extensive use of radio communications than the United States or Western Europe. Most of the territory of the Soviet Union was far north and not conveniently served by synchronous satellites, so the Soviets developed a family of communication satellites, called Molniya, that move in polar orbits. A *Molniya orbit* passes over the Northern Hemisphere at very high altitude and thus moves quite slowly during this part of its journey. Its perigee, in contrast, is low over the Southern Hemisphere, and that part of the trip goes very quickly. The result is that most of the time the satellite “hangs” above the Northern Hemisphere, where it can be used for high-latitude communications. In order to spy on these communications, the US built satellites, called Jumpseat, that move in Molniya orbits. These satellites are in a position to listen to both radio transmissions from the ground and those from Molniya satellites.

Communications intelligence depends for its success on tactical as well as strategic elements. When an intercept station has been put in the right location, operates at the right time of the day, points its antenna in the right direction, and tunes its radio to the right frequencies, it is rewarded with a flood of traffic too large to record, let alone analyze. The process of examining intercepted traffic to determine what is to be retained and what is not may be as "simple" as detecting which channels within a trunk are active or as complex as recognizing the topic of a conversation. Typical selection processes include active channel detection, called and calling number identification, speaker identification, keyword spotting (in either text or voice), fax recognition, and semantic information processing.

The difficulty of locating and isolating just the right messages is an intrinsic consequence of the volume of traffic in modern communications. Communications intercept equipment must decide in a fraction of a second whether to record a message it has detected or to permit the message to escape. Often it must make the decision to record communications of which it has only one part.[22] If, for example, the two directions of a telephone call are carried on separate facilities, an individual intercept point may have access to only one side of the conversation. Although the entire call may in fact be recorded, so that both sides of the conversation will ultimately be available to an analyst, it will be recorded by two devices acting independently. Should either fail to detect that the call is of interest, and therefore fail to record it, the utility of the other component will be vastly reduced.[23] The problem of identifying traffic of interest among all possible traffic is the problem of *search*.

Communications are organized at many levels. The entities communicating have addresses—in radio these are called *call signs* (commonly known in the case of commercial stations as *call letters*); in the case of telephones they are telephone numbers; in the case of computer networks, they are IP addresses, email addresses, URLs, etc. Messages follow *routes*, which in turn are made up of *links* or *hops* on *trunks*. Within an individual trunk, messages are *multiplexed* into channels, which make up the trunk much as lanes make up a road.[24]

At the lowest level, intercept equipment sits and looks through the space in which messages might be found. At each frequency, or time slot, or code pattern, it listens to see if there is any traffic at all. It may well be the case that most of the channels in a trunk are inactive most of the time.

When intercept equipment detects an active channel, it must decide whether to record what it finds there. This depends on *diagnosis*: characterization of the form and the significance of the signal that has been found. If the channel is a telephone channel, for example, the likely possibilities are voice, fax, and data. The intercept device must try to decide what it is hearing and may then discriminate more carefully depending on the category. The first step will usually be to listen for dial pulses or touch tones and attempt to determine what number is calling and what number is being called. If the call is voice, the device may attempt to determine what language is in use, or even listen for keywords. If the call is fax, it may try to determine whether the transmission is text or pictures. If the call carries data, it will attempt to determine what type of modem is in use and what codes (ASCII, Baudot, EBCDIC) or data formats are present. When text is detected, the equipment may go further and apply semantic processing to determine the subject of the message in much the same way that a search engine tries to locate a topic of interest on the World Wide Web.

One strategy followed by many pieces of intercept equipment should be a caution to anyone using cryptography: if an intercepted message is found to be encrypted, it is automatically recorded. This is possible because at present only a small fraction of the world's communications are encrypted. The first lesson to be drawn from this is that if you encrypt something you had better do it well; otherwise you will only succeed in drawing attention to yourself. The second is that as the use of cryptography increases, the privacy of everyone's traffic benefits.

Once traffic has been diagnosed as interesting, it will be recorded. This is not as simple as it sounds. Typically a signal can be recorded in several different formats, depending on how well it has been understood. It is always possible to make a recording of the waveform being received, but this may turn out to be much bulkier than the message it encodes. For example, recording a modem signal carrying 2400 bits per second of information (about 240 characters a second), without demodulating it, uses up the 48-kilobyte-per-second capacity of a digital audio tape. A direct recording of the signal is thus 20 times the size of the message it contains.

Neither diagnosis, nor recording, nor any form of analysis that may be done on an intercepted signal can be separated from *signal processing*

—study of the signal by mathematical and computational means. Digital signal processing (one of the fastest-growing areas in computing) is revolutionizing communications. The availability of $100 modems is a consequence of the availability of signal-processing chips costing a few dollars apiece.

Demodulating modem signals (which accounts for most of the signal processing in data interception) is far harder for an intercept device than for the modems used by the sender and the receiver. Present-day modems go through a period of training at the beginning of a call during which they study the communications path and "discuss" how best to make use of it. Even if the intercept device is listening to this "conversation," it cannot transmit without revealing its presence, and thus it cannot engage in the negotiations. The signal quality available to the intercept device is therefore rarely as good as that available to the communicating modems.

Only after traffic has been located, demodulated, and recorded do we finally get to the most famous process in communications intelligence, the process of breaking codes: *cryptanalysis*. This book is not the place for a technical discussion of cryptanalysis; such discussions now abound in both the technical and the historical literature of cryptography.[25] It is, however, the place for a discussion of the process of cryptanalysis.

Most of the public literature, both technical and historical, is devoted to *research cryptanalysis*, the process of breaking codes for the first time. This is naturally an indispensable component of any production cryptanalytic organization, but does not account for most of its budget or most of its personnel.[26] The object of "codebreaking" is the development of *methods* that can be applied to intercepted traffic to produce plaintext. In modern cryptanalysis, this is often done entirely by computers, without human intervention.[27]

The process of converting ciphertext to plaintext is called *exploitation*. It follows a process of *diagnosis* closely related to the more general diagnosis of traffic discussed above.

The heart of a communications intelligence organization, however, is not cryptanalysis but *traffic analysis*—study of the overall characteristics (length, timing, addressing, frequencies, modulation, etc.) of communications.[28] Traffic analysis by itself provides a broad picture of the activities of communicating organizations (Wright 1987). One of NSA's most noteworthy lapses was its failure to detect India's preparations for its nuclear tests in 1998—a failure to detect increased traffic around Pokharan, southwest of New Delhi, where the tests were conducted.

Moreover, it is essential to assessing the signaling plan, the traffic patterns, and the relationships among communicating entities. Elaborate databases of observed traffic (Hersh 1986, pp. 258–259) underlie all COMINT activities.

A last operational point that bedevils communications intelligence is *retention*—the preservation of intercepted signals for short or long periods of time until they can be processed, cryptanalyzed, interpreted, or used. As we have noted, storing a signal that the holder is unable to restore to its original form typically takes far more memory than storing an understandable signal. This is justified because, enciphered messages can be of value even if they are first read only months or years after they were originally sent. During World War II, Allied cryptanalysts were sometimes weeks or even months behind on some classes of traffic (Welchman 1982). Some signals intercepted during the Cuban missile crisis of 1962 were not read until 2 years later (Hersh 1987). In what is probably the granddaddy of ciphertext longevity, Soviet messages sent in the 1940s were still being studied in the 1970s (Wright 1987). Managing the storage of intercepted material is thus a major problem in all signals intelligence activities.

After all of the technical processes characteristic of communications intelligence, the *product* enters into the part of the process common to information from all intelligence sources: interpretation, evaluation, dissemination. One process looms larger over COMINT than over perhaps any other intelligence material: *sanitization*—removal from the intelligence product of information that would reveal its source. Sanitization to greater or lesser degrees produces intelligence of varying levels of classification.[29]

Secrecy in Communications Intelligence

It is impossible to exaggerate the importance of security to every phase of communications intelligence. In other areas of military activity, secrecy plays an important role but is rarely indispensable to success. A superior army often vanquishes its adversary despite lacking the element of surprise. Even in the area of nuclear weapons (where it abounds), secrecy serves primarily to prevent proliferation. If all of America's nuclear secrets were to be published tomorrow, nuclear weapons would remain just as destructive as they are today and almost as effective as weapons of war. In contrast, communications intelligence would be rendered significantly less effective by disclosure of its techniques and capabilities. Even a credible warning to an opponent that its communications are being intercepted and exploited can result in the opponent's taking action to restore the security of its communications and can destroy the results of many years of intelligence work.[30]

Once traffic has been identified and recorded, shipping it home for further analysis presents security problems of its own. If the intelligence is needed promptly, telecommunication channels must be used. The traffic is, of course, encrypted to conceal from the opponent the details of what is being recorded, if not the fact of interception itself. The circumstances, however, give the opponent a measure of control over what is transmitted on the channel and may provide the opportunity for a chosen-plaintext attack (see chapter 2) on the cryptography. Moreover, unless careful measures are taken to counter traffic flow analysis, correlation is likely to reveal much detail of the interceptors' activities to the opponent.[31]

Current Status of the COMINT Product

Communications intelligence is enjoying a golden age.[32] The steady migration of communications from older, less accessible media—both physical and electronic—has been the dominant factor. The loss of information resulting from improvements in security has been consistently outweighed by the increased volume and quality of information available. As a result, COMINT has been improving for more than 50 years and has become a growth industry.

Even 50 years of success has not made the supporters of COMINT confident that the success will continue, however. From the beginnings of the multinational arms buildup that followed World War II, there have been repeated warnings that improvements in cryptography would bring about the demise of communications intelligence. After the emergence of a public cryptographic technology in the late 1970s, these warnings became especially shrill and were joined by self-confident predictions from the academic and commercial cryptographers that they could produce unbreakable systems and that this would put NSA and its cousins out of business.[33]

The independent cryptographers may well have been correct in their technical bravado but entirely wrong in their view of its consequences. Equating unbreakable cryptography with the security of communications is like equating cryptanalysis with signals intelligence.

It is often said that the intelligence agencies of the major powers can no longer break each other's high-grade systems and must subsist on reading the traffic of Third World countries (Simmons 1986). Although the intelligence community itself has done all it can to foster this view, the steady expansion of COMINT facilities[34] suggests it is too modest.

The status of cryptanalysis in the contemporary world is hard to determine, owing to pervasive secrecy. Oddly enough, although the "Russian Project" is the most secret of NSA's secrets, the fortunes of an activity this important are hard to conceal. What evidence there is makes it plausible that high-grade Russian traffic continued to be read at least until the early 1980s and may still be accessible today.

In its early years, the Soviet Union, like most of the world at that time, relied on code books to secure its military and diplomatic communications. This practice appears to have come to an end in 1927 with MI5's raid on the London offices of the All-Russian Cooperative Society and with the prime minister's admission in Parliament that Britain had been reading Soviet messages for years. It is presumably at that point that the Russians began the extensive reliance on one-time systems that was long characteristic of their operations. In the 1930s and the 1940s their use in Soviet diplomatic communications seems to have strained the facilities for key production to the breaking point, and they began to reuse keying material. Despite the subtle worldwide pattern of the reuse, it resulted in some of their most sensitive messages' being read (Wright 1987). Discovery of this fact after World War II must have led to a broad program to improve the security of Soviet communications.[35]

The Russians were undoubtedly aware of rotor machines and other mechanical cipher equipment as early as the 1920s, but they seem not to have made much use of this awareness before the end of World War II. With their capture of the eastern part of Germany and the acquisition of many of the papers of Pers Z (probably the best of the German cryptanalytic organizations; see Kahn 1967), the awareness must have been enhanced, and perhaps their interest was piqued.

In the late 1940s a cryptographic laboratory was established at Marfino, in the suburbs of Moscow. The focus of its efforts was secure telephones, of which it produced several, some analog and some digital.[36]

If developments in the Soviet Union followed a course similar to those in the West, rotor machines could comfortably operate at teletype speeds of 50–110 bits per second (bps), but could not keep up with the 2400 bps and higher needed for digitized voice. This led to the development of purely electronic shift-register systems, although rotor machines remained in use for text traffic for many years thereafter.

In the late 1950s, according to Peter Wright (1987, p. 148), NSA and its British counterpart, the Government Communications Headquarters (GCHQ), jointly mounted an attack on a Russian machine they called "Albatross." Development cycles in cryptography are long, and at that date this was probably a rotor machine. Wright makes no concrete statement about the success or failure of the project, but the self-congratulatory tone in which he describes pushing the endeavor suggests success.[37]

Traffic encrypted by Soviet cipher machines was also read by the Americans during the 1960s. The messages, encrypted in a Soviet cryptosystem which NSA code-named *Silver*, played a prominent role in a 25th-anniversary post mortem of the Cuban missile crisis, held at Harvard University, at which it was revealed that for several hours the Cubans had taken control of a Soviet military base and of some of the nuclear missiles. NSA was not able to read the traffic at the time it was sent; it only became aware of this critical new dimension of the crisis when the messages were first read in 1964.

In their analysis of a number of spy cases from the 1970s, Corson et al. (1989, pp. 94–95) refer to an "NSA intercept from the Soviet Embassy in Washington in April 1977." They go on to say: "The cable was sent by Ambassador Anatoly Dobrynin to the Foreign Ministry in Moscow. It referred to advice Henry Kissinger had given Dobrynin on how to deal with the new Carter administration in the ongoing SALT II negotiation." (ibid., 1989, pp. 94–95) It strains credulity to suppose that such a telegram would have been sent in clear. If the telegram was intercepted by NSA, it must have been cryptanalyzed. The process by which the authenticity of the cable was established lends further weight to this view. The CIA officers involved are quoted as saying that "the only way to confirm the authenticity of the cable was to go out to NSA, pull the transcripts of other cables sent from the Soviet Embassy, and compare the style, content, and timing." As a result, "the experts at NSA concluded that the cable was real and not a Soviet disinformation effort" (ibid., pp. 97–98). This information is all the more persuasive because the authors mention "intercepts" without appearing to have given any thought to cryptography. Their concern is entirely with the content of the cable and its implications about the propriety or impropriety of Kissinger's relationship with Dobrynin.

Evidence of still more recent US success in reading high-level Soviet traffic arises in connection with the September 1983 destruction of Korean Airlines 007. Seymour Hersh's book on the subject describes the interception of a call from Khabarovsk to Moscow placed via the Soviet Raduga satellite and intercepted by the US Jumpseat satellite—which had been placed in a similar orbit for just that purpose. Hersh (1986, p. 232) quotes an unnamed NSA official as saying that "the cipher signal snapped on and some long-precedence message was sent." He remarks that the "NSA officials would not say anything further about the message." Others were more forthcoming, including a senior US intelligence officer who "vividly recalled his reaction well after the shootdown of Flight 007, upon being shown a copy of the deputy commander's intercepted and decoded message to Sakhalin."

The most recent evidence of the continuing success of cryptanalysis involves Iranian communications. Ahmad Chalabi, a Shiite member of the Iraqi government and a founder of the Iraqi National Congress, was accused of leaking to the Iranian government the fact that the US was able to read diplomatic traffic between Teheran and its embassy in Baghdad. No credible explanation of how Chalabi would have known this with any certainty has been put forward, and it appears more likely that the real leak came from the US government. In an effort to discredit Chalabi, who had fallen out of favor in its eyes, the US released an intercepted diplomatic cable quoting Chalabi's warning—solid evidence that, whether the

Iranians had previously known it or not, the US was reading Iranian traffic (Galbraith 2006, p. 30). [Disclosure: Chalabi and Diffie studied mathematics together at MIT from 1961 to 1965.]

Non-Cryptographic Impediments to Interception

If cryptography has not stopped communications intelligence, other developments must at least have slowed it down. In recent decades, the loss of intelligence resulting from the use of cryptography to protect communications appears to have been eclipsed by losses due to other developments not intended primarily for security. These include optical fiber, high-speed modems, and dynamically routed communications.

Between World War II and the appearance of optical fiber, the major developments in transmission technology had the effect of rendering communications more vulnerable to interception. Microwave relays were more accessible than the copper wires they replaced, and satellite channels were more accessible still. Optical fiber, on the other hand, is directly competitive with these radio technologies in cost and bandwidth, and immeasurably more secure. Although undetectable taps on unprotected fiber circuits are possible, they always require physical contact, which is often infeasible. Owing to its economic advantages, optical fiber has been used to reduce the vulnerability of US communications and those of other nations around the world.[38]

A more interesting signal-acquisition problem has arisen out of improvements in modem technology. For decades, Telex and similar low-speed data-communication facilities were the backbone of both commercial and government communications in most of the world. Data rates increased gradually from 50 bits per second to 75 to 110 to 150, and finally to 300. Around 1980, the speeds of inexpensive modems jumped to 1200 bps. Today, they are 28,800 bps.[39] Since the older modems acted essentially independently, each using a phase-locked loop to interpret a set of data pulses in relation to a predictable timing pulse, an intercept modem had no difficulty in doing exactly the same thing.

The new modems not only indulge in initial training to optimize their use of particular communication circuits; they also employ autocancellation: both modems transmit simultaneously on the same set of frequencies, and each subtracts its own transmission from the signal it is receiving.[40] Even at 2400 bps, this presents serious difficulties for a passive intercept device attempting to separate the two halves of the signal. At 4800 bps, 9600 bps, and higher, the problem becomes progressively more difficult. Furthermore, it appears to be, in a sense, intrinsic. If the intruding modem can separate and interpret the two data streams, it is receiving information twice as fast as the "legitimate" modems. This suggests that a modem using the same techniques as the intercept device could operate twice as fast. In many cases, the development of the technology of communications and that of communications intelligence proceed independently or even synergistically. In the case of modems, improving technology works directly, if unintentionally, against interception.

The increasing difficulty of acquiring modem signals goes hand in hand with another trend in modern communications: better modems have led to an explosion in the use of dialed-up point-to-point connections to replace leased lines. Private networks often use the same circuits month after month or even year after year. Once such a network has been mapped and access points located, the same intercept facilities can be employed for long periods of time. Furthermore, the ownership of such a net typically determines much about the traffic it carries, which drastically reduces the need for further filtering. In contrast, dialed-up point-to-point connections must be identified within the larger traffic volume of a common carrier's network. This is complicated by *dynamic routing*.[41] Even after it has been determined that a high fraction of the traffic between two particular telephone numbers is worth targeting, it may be difficult to acquire this traffic because different circuits are established on different calls.

The impact of dynamic routing has in some measure been mitigated by commercial developments. The Internet today is intended less to survive a nuclear attack than to serve the needs of millions of customers moving trillions of bits. For the most part, its facilities are owned by a small number of large communications carriers who handle packets by a strategy known as *hot-potato routing*: when you get a packet you try to hand it to the network that owns the destination as quickly as possible. In practice this means that communication between parties on two different networks will be carried on one of two channels, depending on which direction it is going. An intercept facility placed in an appropriate position will have access to a large body of material and will not have to contend with packets following a wide variety of paths.

A related development in switching systems, common-channel signaling (the practice of sending signaling information out of band in a separate digital signaling channel), can be both a blessing and a curse to the interceptor. It is a blessing in that it gathers together in one place the calling number, the called number, and the way the call is to be handled and routed. It is a curse because the common channel can be routed more securely—through copper or fiber, or on an encrypted channel.[42] If this is done, the call itself carries no identifying information and becomes difficult for an opponent to locate. This characteristic makes it possible to upgrade an existing wire-line communication system to a radio-based system of a much higher capacity with little loss of security. All signaling is routed through the pre-existing (and more secure) wires to minimize the vulnerability of the radio circuits.

The Impact of Encryption on Communications Intelligence

Although the spread of encryption technology is not at present the most serious cause of lost communications intelligence, its potential impact on intelligence activities should not be underestimated. Many of today's secure telephones require the users to secure the call as a distinct action from making the call. The process takes 10–20 seconds—long enough to be a deterrent to doing it at all. The digitized voice is of lower quality and may exaggerate other unpleasant phenomena, such as line noise. The callers are likely to say at least a few words to each other before initiating security. If the message is short enough and seems innocuous, they may not bother with security at all. All this leaves room for various sorts of information leakage.

The Integrated Services Digital Network (ISDN)—a set of telephone standards for direct digital telephone service—potentially alleviates the problems of POTS-oriented secure phones.[43] The time required to initiate a secure call drops to under a second and encryption has no effect on voice quality since the signal is digitized in any case. Should ISDN fulfill its promise to permit digital end-to-end negotiation before the called phone rings, the need to initiate security explicitly will be eliminated and the result will be a form of secure caller ID.

The future of voice telephony is Internet telephony, Voice over IP, which lends itself even more readily to full automation than ISDN. Skype, one popular VoIP system, automatically encrypts all calls between Internet clients.[44]

Extensive use of link encryption can also have devastating effects on intelligence gathering. When link encryption is applied to microwave beams and to satellite channels, it conceals everything passing over them; the intruder sees nothing but a steady flow of random data that does not even reveal whether real communication is taking place. Typically, however, link encryption cannot be applied by the users and must be supplied by the carrier. Link encryption will therefore provide users with protection against some spies but not others. In a world with an ever-growing number of interconnected and competing communications carriers, this opens numerous opportunities to couple communications intelligence with human intelligence and network penetration.

Despite the possibilities, the vast majority of the world's traffic is currently in plaintext.[45] This makes it feasible to sort traffic in real time to determine which messages are of interest and which are not. On circuits where the fraction of ciphertext is not too high, the fact of encryption itself provides a valuable clue to the potential significance of intercepted material.

Combined with the limited use of encryption is the diversity of cryptographic products in use throughout the world. The relatively small fraction of traffic that is encrypted today is encrypted in a wide variety of cryptographic systems. This enables interceptors to recognize traffic by identifying the encryption techniques or equipment used. This *diagnosis* of cryptosystems need not require cryptanalysis or cryptomathematical statistics. Distinct cryptosystems typically employ different data formats that can easily be distinguished, and it is desirable from the COMINT viewpoint to preserve those characteristics of communications that permit the filtering of traffic and the selection of messages.

The rise of international encryption standards, even de facto standards, may make this task immeasurably more difficult. We will have more to say about twenty-first-century cryptography in chapters 10 and 11.

One of the distinguishing characteristics of cryptography is that it is robust. Much cryptographic equipment is located close to its users and is likely to survive any attack that does not destroy the users themselves. Cables and optical fibers, like roads and railways, are vulnerable to attack all along their lengths.

The first British military action of World War I was the cutting of an undersea cable, which forced the Germans to use radio for messages to North America and made their communications vulnerable to interception (Kahn 1967, p. 266). Similar scenarios were played out during the Normandy invasion in World War II[46] and at the start of the first Gulf War.[47]

The impact of encryption (and other technical developments) on the interceptor depends very much on the interceptor's position. If the surveillance is entirely external, pointing even the fanciest antennas at the target, a comprehensive program of radio encryption will defeat it. If the surveillance is internal, built into the communications infrastructure for any of a variety of possible purposes, it will be inside this layer of encryption and little affected by it. This has two important consequences. First, it is very difficult for any individual or group within a society to protect its communications comprehensively. It can make use of end-to-end encryption but this will leave the pattern of communications visible. Any greater degree of protection, such as anonymity services, requires the society's cooperation or at least tolerance. Second, it points up the sensitivity of any monitoring capability built into a communication system. By design, the monitoring system will bypass most of the investment in security against external opponents. It will itself become the target and will be especially vulnerable to insider attacks. Security must therefore be a primary consideration in the construction of any such system.

Information Warfare

The meaning of the term "information warfare" is far from settled and the term is applied to subjects that range from modern but established military practice to complete science fiction. In one of its solider embodiments, information warfare is the management of information in warfare. In World War II, pilots would receive intelligence information in a pre-flight briefing; during the mission they would get no new information except for what they could see with their own eyes and an occasional radio message. Today, however, fighter and bomber pilots are assisted from takeoff to landing by the products of a real-time intelligence machine that integrates information from signals intelligence, satellites, surveillance aircraft, and other combatants. It will tell them whether the targets for which they set out have already been destroyed, whether interceptors have scrambled to meet them, or whether previously concealed anti-aircraft batteries have become active and present a threat. It is one of the major objectives of the modern military to close its information-processing loop, bringing observation, decision, and action closer together. The first Gulf War was both a test bed for and a triumph of this approach, which is now solidly established in American military doctrine (Campen 1993a).

Where information processing is an essential military tool, it will naturally be subject to attack. Radar installations are now vulnerable to missiles that follow a radar beam and destroy its source,[48] and much recent military thinking has gone to improving strategies for attacking communication facilities and surveillance aircraft. The possibilities include frying computers with high-power microwaves and shorting them out with carbon fibers.[49] Some attacks on information resources are meant not to destroy them but merely to render them temporarily ineffective. This aspect of information warfare is an outgrowth of the established field of electronic warfare, in which radio and radar are pitted against jamming,[50] decoys, and chaff.

Discussions of this sort are real enough and genuinely high-tech, but in a sense unimaginative. The heart of information warfare today is the notion of attacking the enemy with information alone. This idea is not entirely new. In classical warfare it is called propaganda and disinformation. A less classical antecedent is the practice of communications deception: making use of the opponents' own signals intelligence activities to fool them.[51]

The present-day concept is rooted in the essential role of information not just in battle but in all aspects of society. An opponent who is critically dependent on information will be catastrophically vulnerable to corruption of that information. The notion has been enveloped in an apocalyptic aura by the development of *viruses* and *worms*[52]—malignant forms of software that reproduce within an opponent's computers and eventually cause them to malfunction. Computer viruses originated as a malicious prank and are now a widespread hazard of the computer world.[53] The military vision is that by the application of millions of dollars and hundreds of people far more subtle forms of viruses, suitable as weapons in military conflicts, can be developed.[54]

The impact of such invaders has already been quite noticeable. One incident brought down a telephone "loop carrier" switching system, disabled the tower at the Worcester Airport and shutting down the airport for six hours (Festa 1998). An attack on a sewage treatment plant in Maroochy Shire, Australia resulted in the release of thousands of gallons of untreated sewage (Shea 2003). A safety monitoring system at the Davis-Besse nuclear power plant was disabled by the Slammer worm. Fortunately, the plant was off at the time and there was no immediate hazard. The worm had bypassed the plant's firewall by entering through a machine on the unsecured network of a contractor (Poulsen 2003).

Computer Intelligence

One aspect of information warfare that is unquestionably real, though how much of it is occurring is hard to assess, is the practice of obtaining information by active intrusion into a target's computers or networks. We shall call this field *computer intelligence*.

Both the strengths and the weaknesses of communications intelligence derive from the fact that it is passive. On one hand, its passive character means that communication spies are rarely caught. On the other, its passivity deprives it of the chance to go after particular pieces of information and restricts it to listening to what opponents decide to transmit. This raises the cost of interception by obliging the interceptors to winnow through vast quantities of traffic in order to find what they want to know. A passive eavesdropper must wait for some legitimate user to access the information and then record the result; an active one can go to a database and extract a particular piece of information.

Intrusions into American computers by a group in Germany with ties to the KGB are described in a 1989 book by Clifford Stoll. An operation in Tripoli by the Israeli Mossad provides an interesting example of the intersection between human intelligence and the low-tech end of network intelligence. Using a phone line that actually originated in Israel but appeared to originate in France,[55] and masquerading as French shipping insurers, the Mossad recruited the harbormaster in Tripoli and "ran" him for more than 2 years (Ostrovsky 1990, chapter 16). With the worldwide linking of computers through the Internet, new techniques for extracting information by active penetration are at the frontier of intelligence research (Schweizer 1993, pp. 158–163) and are being developed all over the world.

At a meeting on information warfare at Stanford University, members of the President's Commission on Information Warfare and Critical Infrastructure Protection acknowledged that there has not yet been an example of information warfare in its pure form. No nation has attacked another nation's computers using information. Nor is it believed that a politically motivated attack on computers using information alone has been made by terrorists or other non-national groups. Nonetheless, information warfare is very real, and very alive as a subject of military speculation, planning, and development. Not a month passes without a conference, meeting, or war game devoted to the subject.

In the late 1990s, these issues appeared to be largely theoretical. They are no longer. It is clear that the Chinese government has "invested significantly in cyberwarfare training and technology" (Kaplan 2005, p. 54). Japan has already suffered a number of attacks originating in China and South Korea (Faiola 2005). Japan is not alone. The US has also been targeted.

"China has downloaded 10 to 20 terabytes of data from the NIPRNet [The Department of Defense's Non-Classified IP Router Network]," Major General William Lord, director of information, services and integration in the Air Force Office of Warfighting Integration and Chief Information Officer, reported in 2006.[56] We have evidence of clear and highly targeted attacks. For example, the following set of attacks sought military computers that had specific known vulnerabilities:

- "At 10:23 P.M. PST, [attackers] found vulnerabilities in computers at the US Army Information Systems Engineering Command at Fort Huachuca, Arizona.

- At 1:19 A.M. PST, they found the same hole in computers at the military's Defense Information Systems Agency in Arlington, Virginia.

- At 3:25 A.M. they hit the Naval Ocean Systems Center, a defense department installation in San Diego, California.

- At 4:46 A.M. PST, they struck the United States Army Space and Strategic Defense installation in Huntsville, Alabama." (Thornburgh 2006a)

Of course, we do not know for sure that these files were stolen by the Chinese military. But what we do know would surely indicate that. We know the files were "zipped" and immediately transmitted to computers in South Korea, Hong Kong, or Taiwan, and then to the People's Republic of China. Attacks were fast: in and out of the targeted computers in 10–30 minutes. And, most telling to government investigators, "these guys never hit a wrong key" (Thornburgh 2006b).

We also know some things that have been taken: specifications for the aviation mission-planning system for Army helicopters from the Army Aviation and Missile Command and Falconview 3.2, the flight-planning software used by the Army and Air Force (Espiner 2005).

On balance, the Department of Defense takes the security of its networks—even its unclassified networks—more seriously than do most corporations. If penetration on this scale could happen to a military network, it seems prudent to assume that it is also happening to civilian networks.

The relevance of information warfare to cryptographic policy is twofold and straightforward. The major worry of most pundits is that critical elements of national infrastructures such as transportation systems and power grids are being connected to control systems that communicate via the Internet. Much of the plausibility of this concern lies in the lack of authentication in current computer networks. Viruses might get in because new versions of programs are loaded over the Internet, and there is no easy way of telling a genuine program from an alternate one prepared by intruders. Furthermore, the information that opponents would need to mount an attack is available as a result of the general lack of security in communications. Widespread deployment of cryptography in the "command and control" of the civilian infrastructure would solve both problems.

The Relationship of Security and Intelligence

In loose correspondence with the various categories of intelligence are security measures intended to counter them and limit their effectiveness. Thus, for example, human intelligence can be countered by limiting information access to vetted personnel, photographic intelligence can be countered by camouflage, and open-source intelligence can be countered by restricting public access to information or mixing false information with genuine.[57] Cryptography is the centerpiece of communication security, the countermeasure to communications intelligence.

As with the various aspects of intelligence, security measures are far from independent. For example, good personnel security is essential to communication security, and communication security can in turn make a major improvement in operations security.

The Security of Communications in the United States

No nation in the world is more dependent on electronic communications than the United States. As a result, no nation is more vulnerable to subversion of its commerce, its money supply, and its civic functions by electronic intruders. Attempts to address this vulnerability take two forms:

- Protecting American communications by government action in the same way that the country as a whole is protected by defense and law-enforcement agencies.
- Leaving the protection of most communications to the private sector and encouraging such protection by such measures as standards, incentives, and regulation. This parallels the way in which physical security is provided by locks and alarm systems in civil society, often in consideration of reduced insurance premiums.

In practice, any comprehensive solution must have elements of both.

In the 1970s, the US government made its first attempts to secure broad segments of American communication rather than narrow classes of military, diplomatic, and intelligence traffic. Some communications (in Washington, New York, San Francisco, and other areas that harbored Soviet diplomatic or consular facilities) were routed through underground cables rather than over microwave relays, analog and digital encryption devices were developed for the protection of telephone trunk lines,[58] the security of common-channel interoffice signaling was improved,[59] and telephone satellite channels were encrypted.

With the demise of the Soviet Union, whose hostility to the United States was supported by a massive intercept capability, and with the migration of more and more of our critical infrastructure to Internet- and Web-based mechanisms, the focus of our concerns has shifted from passive intercept to active attack. In the process, national security and commercial security have become intertwined.

For most purposes, the Internet is the most effective and economical communications medium in the world, and businesses have been quick to improve their functioning and lower their expenses by taking advantage of it. The flexibility and worldwide ubiquity of the Internet have also made it an ideal culture medium for a variety of activities that threaten the security of both critical and commercial infrastructure.

The threats can be loosely categorized into a half a dozen forms:

- Break-ins to websites—Most businesses have customer-facing websites that advertise their wares, allow communication with their employees, and perform other functions. Competitors, detractors, and customers may all find ways of interacting with the website that are not what the provider had hoped for. Extraction of more information than the provider intended to provide frequently goes unnoticed, but defacements or perversions of function can cause the website provider embarrassment and financial loss.

- Viruses and worms are an automated form of computer penetration that can be spread by almost any form of computer communication and have shown tremendous destructive potential.

- Denials of service—When opponents cannot break into a website, they may still be able to mount an attack that prevents it from functioning correctly. Such attacks quickly developed the sophisticated technique of capturing less-well-protected computers and turning them into *zombies*. The zombies are woven together into a *botnet* and used to attack particular targets, a technique called *distributed denial of service*.

- *Spam*—Email on the Internet is billed not by the message or by the bit but by the month. There is no disincentive to sending lots of mail. This is analogous to—but even more extreme than—the artificially low bulk mailing rates that support the clutter in our physical mailboxes. Unwanted mail that varies from uninvited to repulsively unwelcome also serves to support other forms of computer malfeasance. Spam can be used to spread viruses and worms, gather information about active email accounts, and commit fraud.
- *Phishing*—Spam uses a number of mechanisms to trick the recipient into providing information that can be used for *identity theft* or other nefarious purposes.
- *Spearing*—Targeted attacks encouraging a small, carefully selected group to install a patch in their security systems. The patch is in fact a vulnerability.

The threats, coupled with the staggering commercial importance of the Internet, have created a new security industry with revenues in the tens of billions of dollars a year. The new industry is more complex than its "purely national security" predecessor. The only defenses against Soviet eavesdropping were proactive. If we failed to prevent them from getting useful information, there was rarely anything we could do after the fact. Commercial security employs a combination of preemptive measures—firewalls, intrusion detection systems, encryption—with forensic and investigative techniques that deter opponents who are more subject to legal retribution than was the Soviet Union.

Our efforts to date, however, fall far short of providing the degree of protection desired in a communications infrastructure that has become indispensable to American prosperity and security.

Federal Policies and Programs

The challenge, from the national-security viewpoint, is to achieve a twofold objective:

- Improve the security of communications and computing within the United States and for US government and commercial activities abroad.
- At the same time, attempt to minimize the impact both on US intelligence activities and on domestic security that could result from having the country's own technology used against it.

This objective is difficult, if not impossible, to achieve by a reactive strategy of permitting events to unfold as they will and responding to them piecemeal. Threats to American intelligence capacity, both domestic and foreign, can be anticipated, and policies can be developed to nullify them. Only a misplaced sense of fair play would demand that threats to American well-being should be allowed to develop freely when the means to control them are at hand.

Export Controls

Most of the federal activities discussed so far do not affect the public directly. For one thing they are secret. When foreign policy is successful, people who give the subject some thought may attribute a share of the success to intelligence. When the United States is surprised by something —like the taking of the hostages in Iran, the Iraqi invasion of Kuwait, or the attacks of 9/11—poor intelligence is likely to be blamed. Intelligence has, however, no visible day-to-day impact on the lives of most Americans.

There are, however, federal activities in support of intelligence that affect many people—usually, as those people see it, adversely. These are the export-control laws. Although the US Constitution prohibits export tariffs, it does not prohibit an outright ban on exporting particular things to particular countries.

All exports from the United States are regulated under one of two laws: the Arms Export Control Act (22 U.S.C. 2571–2794) and the Export Administration Act (50 U.S.C. App. 2401–2420). The Arms Export Control

Act takes precedence over the Export Administration Act and confers on the Department of State the authority to regulate the export of anything it deems to be a weapon of war (or, as the export laws term it, a *munition*). Items ruled to be munitions require individually approved export licenses designating the customer, the application, and often conditions for the handling or redeployment of the item.

Things that are not munitions but that may have military applications are called *dual-use items*. If the Department of State decides that something is a dual-use item, it transfers jurisdiction over its export to the Department of Commerce, which administers the Export Administration Act. Under the Export Administration Act, exporters can receive licenses to export to broad classes of customers in broad regions of the world. In the area of cryptography, for example, equipment using the Data Encryption Standard to authenticate bank-to-bank wire transactions was allowed to be exported to banks in most countries in the world even when export of comparable equipment for other applications was not. Under the Export Administration Act, furthermore, the Department of Commerce is obliged to take into account the foreign availability of equivalent products[60] in deciding whether to grant or deny an export permit—that is to say that it can block exports only where there is evidence that such action is actually likely to prevent a foreign customer from acquiring a product with equivalent capabilities. Under the Arms Export Control Act, no such test of foreign availability is required. All cryptographic devices that do not fall into certain narrow categories are regulated as munitions and require individually approved licenses.

Many of the actions of the export-control authorities seemed ludicrous and inspired widespread resentment. In 1994, Philip Karn, a security engineer at the cellular telephone maker Qualcomm, applied for a license to export a copy of Bruce Schneier's popular book *Applied Cryptography*. The license was granted, and the accompanying letter stated that the Department of State did not have authority over published material—a view commendably in accord with the First Amendment. Karn then applied for an export permit for a small part of Schneier's book—an appendix containing source code for cryptographic algorithms—transcribed onto a floppy disk, rather than on paper. That application was denied. This case, which is working its way through the federal courts, has made the export-control regime an object of ridicule, but the cryptographic export policies of the United States may appear less foolish and irrational when examined in light of communications intelligence practices.

One natural objective of cryptographic export control is to limit foreign availability of cryptographic systems of *strategic capability*—those capable of resisting concerted cryptanalysis by US intelligence agencies. Were this the only objective, export control in the cryptographic area would be much like export control in other areas—items that have only military uses or have been explicitly adapted to military applications would be treated as munitions, others would not.[61]

Probably the most important objective of the export-control regime in the area of cryptography is to slow the widespread deployment of cryptographic systems of sufficient strength to present a serious barrier to traffic selection. Rather than limiting the export of cryptosystems whose traffic would take weeks, months, or years to break, the objective is to prevent the export of cryptosystems that cannot be broken in real time by intercept equipment in the field. This is a far lower bar, and it precludes the export of any system that could reasonably be said to provide acceptable security for most commercial applications.[62]

It also appears to have been an objective of export control—and, if so, one that had remarkable success—to prevent widespread adoption of standard cryptographic systems. The development of standards would be expected to have two effects from an intelligence viewpoint. It would expand the use of cryptography, thereby complicating both traffic selection and exploitation. It could also result in a uniform appearance of broad categories of messages, making the problem of selection harder still.

More recently, US policy has shifted from suppressing to promoting standard cryptosystems. This change will be explored in subsequent chapters.

A final objective of export control goes virtually unnoticed. It is to maintain an ongoing assessment of the quality, availability, and functioning of commercially supplied cryptographic equipment. Would-be exporters are required to disclose the details of their products to the government on a routine basis. Even if they are not obliged to modify their products in order to get export approval, this guarantees that NSA will have the details of each product's functioning on file. The process of acquiring information on how cryptographic products work is thereby separated from any actual occasion on which their traffic is being intercepted, thus contributing to security. From this point of view, a product exported under an export-control permit is entirely different from and far preferable to one exported without any permit or any reporting requirement.[63]

By limiting the strength of exportable cryptosystems to well below what the users felt they needed, export control created a direct conflict between the needs of the government and the needs of commercial and private cryptographic users. It is an oft-expressed opinion that commercial communications do not require the same level of protection as military communications. This is probably more a reflection of the fact that the military are aware of who their opponents are and of the level of effort that these opponents put into attacking them than a reflection of the value of the communications. The communications of commercial organizations are often worth hundreds of millions of dollars,[64] and many industrial secrets, along with much personal and personnel information, have long lifetimes. Air traffic control, power grid regulation, and control of communication networks are essential to the working of society; their disruption would expose participating corporations to immense liabilities and might cost lives as well as dollars.

Cryptographic keys are often held to be the most sensitive of all secrets, because anyone who has access to the keys can gain access to all other secrets (Clark 1986, p. 11-1313). In a “flipside” to this vision, controlling the export of cryptography was seen as essential to controlling the export of information in general. With the increasing importance of intellectual property to modern commerce, it was thought that if smugglers had access to encrypted communications, the export of any form of information would become impossible to regulate and the United States would lose all control of its “electronic borders.” Cipherpunk talk of crypto-anarchy did little to allay the government’s fears.

Fortunately, the attitudes toward cryptography that characterized the Cold War and its immediate aftermath have begun to change. As we will examine in the latter chapters, export controls have been relaxed, and high-grade cryptography has been adopted in national standards. These developments hold promise of the more harmonious relationship between national security and commercial security that the modern world requires.