CHAPTER 16

Electronic and Information Warfare

All warfare is based on deception . . . hold out baits to entice the enemy. Feign disorder, and crush him.
—SUN TZU, *THE ART OF WAR*, 1.18–20

Force, and Fraud, are in warre the two Cardinal Virtues.
—THOMAS HOBBES

16.1 Introduction

For decades, electronic warfare has been a separate subject from computer security, even though they have some common technologies (such as cryptography). This is starting to change as elements of the two disciplines fuse to form the new subject of information warfare. The military's embrace of information warfare as a slogan over the last years of the twentieth century has established its importance—even if its concepts, theory, and doctrine are still underdeveloped.

There are other reasons why a knowledge of electronic warfare is important to the security professional. Many technologies originally developed for the warrior have been adapted for commercial use, and there are many instructive parallels. In addition, the struggle for control of the electromagnetic spectrum has consumed so many clever people and so many tens of billions of dollars that we find deception strategies and tactics of a unique depth and subtlety. It is the one area of electronic security to have experienced a lengthy period of coevolution of attack and defense involving capable motivated opponents.

Electronic warfare is also our main teacher when it comes to service denial attacks, a topic that computer security people have largely ignored, but that is now center stage thanks to distributed denial-of-service attacks on commercial Web sites. As I develop this discussion I'll try to draw out the parallels. In general, while people say that computer security is about confidentiality, integrity and availability, electronic warfare has this reversed and back-to-front. The priorities are:

1. Denial of service, which includes jamming, mimicry and physical attack.
2. Deception, which may be targeted at automated systems or at people.
3. Exploitation, which includes not just eavesdropping but obtaining any operationally valuable information from the enemy's use of his electronic systems.

16.2 Basics

The goal of electronic warfare is to control the electromagnetic spectrum. It is generally considered to consist of:

- *Electronic attack*, such as jamming enemy communications or radar, and disrupting enemy equipment using high-power microwaves.
- *Electronic protection*, which ranges from designing systems resistant to jamming, through hardening equipment to resist high-power microwave attack, to the destruction of enemy jammers using anti-radiation missiles.
- *Electronic support* which supplies the necessary intelligence and threat recognition to allow effective attack and protection. It allows commanders to search for, identify and locate sources of intentional and unintentional electromagnetic energy.

These definitions are taken from Schleher [677]. The traditional topic of cryptography, namely *communications security* (Comsec), is only a small part of electronic protection, just as it is becoming only a small part of information protection in more general systems. Electronic support includes *signals intelligence* (Sigint), which consists of *communications intelligence* (Comint) and *electronic intelligence* (Elint). The former collects enemy communications, including both message content and traffic data about which units are communicating, while the latter concerns itself with recognizing hostile radars and other non-communicating sources of electromagnetic energy.

Deception is central to electronic attack. The goal is to mislead the enemy by manipulating his perceptions in order to degrade the accuracy of his intelligence and target acquisition. Its effective use depends on clarity about who (or what) is to be deceived, about what and how long, and—where the targets of deception are human—the exploitation of pride, greed, laziness, and other vices. Deception can be extremely cost-effective and is also relevant to commercial systems.

Physical destruction is an important part of the mix; while some enemy sensors and communications links may be neutralized by jamming (*soft kill*), others will often be destroyed (*hard kill*). Successful electronic warfare depends on using the available tools in a coordinated way.

Electronic weapon systems are like other weapons in that there are *sensors*, such as radar, infrared and sonar; *communications* links, which take sensor data to the command and control center; and *output devices* such as jammers, lasers, and so on. I'll discuss the communications system issues first, as they are the most self-contained, then the sensors and associated jammers, and finally other devices such as electromagnetic pulse generators. Once we're done with e-war, we'll look at the lessons we might take over to i-war.

16.3 Communications Systems

Military communications were dominated by physical dispatch until about 1860, then by the telegraph until 1915, and then by the telephone until recently [569]. Nowadays, a typical command and control structure is made up of various tactical and strategic radio networks, that support data, voice, and images, and operate over point-to-point links and broadcast. Without situational awareness and the means to direct forces, the commander is likely to be ineffective. But the need to secure communications is much more pervasive than one might at first realize, and the threats are much more diverse.

- One obvious type of traffic is the communications between fixed sites such as army headquarters and the political leadership. The main threat here is that the cipher security might be penetrated, and the orders, situation reports and so on compromised. This might result from cryptanalysis or—more likely—equipment sabotage, subversion of personnel, or theft of key material. The insertion of deceptive messages may also be a threat in some circumstances. But cipher security will often include protection against traffic analysis (such as by link encryption) as well as of the transmitted message confidentiality and authenticity. The secondary threat is that the link might be disrupted, such as by destruction of cables or relay stations.
- There are more stringent requirements for communications with covert assets such as agents in the field. Here, in addition to cipher security issues, location security is important. The agent will have to take steps to minimize the risk of being caught as a result of communications monitoring. If she sends messages using a medium that the enemy can monitor, such as the public telephone network or radio, then much of her effort may go into frustrating traffic analysis and radio direction finding.
- Tactical communications, such as between HQ and a platoon in the field, also have more stringent (but slightly different) needs. Radio direction finding is still an issue, but jamming may be at least as important; and deliberately deceptive messages may also be a problem. For example, there is equipment that enables an enemy air controller's voice commands to be captured, cut into phonemes and spliced back together into deceptive commands, in order to gain a tactical advantage in air combat [324]. As voice-morphing techniques are developed for commercial use, the risk of spoofing attacks on unprotected communications will increase. Therefore, cipher security may include authenticity as well as confidentiality and/or covertness.
- Control and telemetry communications, such as signals sent from an aircraft to a missile it has just launched, must be protected against jamming and modification. It would also be desirable if they could be covert (so as not to trigger a target aircraft's warning receiver), but that is in tension with the power levels needed to defeat defensive jamming systems.

The protection of communications will require some mix, depending on the circumstances, of content secrecy, authenticity, resistance to traffic analysis and radio direction finding, and resistance to various kinds of jamming. These interact in some rather unobvious ways. For example, one radio designed for use by dissident organizations in Eastern Europe in the early 1980s operated in the radio bands normally occupied by the Voice of America and the BBC World Service—and routinely jammed by the Russians. The idea was that unless the Russians were prepared to turn off their jammers, they would have great difficulty doing direction finding.

Attack also generally requires a combination of techniques, even where the objective is not analysis or direction finding but simply denial of service. Owen Lewis summed it up succinctly: according to Soviet doctrine, a comprehensive and successful attack on a military communications infrastructure would involve destroying one third of it physically, denying effective use of a second third through techniques such as jamming, trojans or deception, and then allowing one's adversary to disable the remaining third in attempting to pass all his traffic over a third of the installed capacity [500]. This applies even in guerilla wars: in Malaya, Kenya, and Cyprus, the rebels managed to degrade the telephone system enough to force the police to set up radio nets [569].

In the 1980s, NATO developed a comparable doctrine, called *Counter-Command, Control and Communications* operations (C-C3, pronounced C cubed). It achieved its first flowering in the Gulf War; the command and control systems used there are described in [643]. (Of course, attacking an army's command structures is much older than that; it's a basic principle to shoot at an officer before shooting at his men.)

16.3.1 Signals Intelligence Techniques

Before communications can be attacked, the enemy's network must be mapped. The most expensive and critical task in signals intelligence is identifying and extracting the interesting material from the cacophony of radio signals and the huge mass of traffic on systems such as the telephone network and the Internet. The technologies in use are extensive and largely classified, but some aspects are public.

In the case of radio signals, communications intelligence agencies use receiving equipment, that can recognize a huge variety of signal types, to maintain extensive databases of signals—which stations or services use which frequencies. In many cases, it is possible to identify individual equipment by signal analysis. The clues can include any unintentional frequency modulation, the shape of the transmitter turn-on transient, the precise center frequency, and the final-stage amplifier harmonics. This *RF fingerprinting* technology was declassified in the mid-1990s for use in identifying cloned cellular telephones, where its makers claim a 95% success rate [341, 677]. It is the direct descendant of the World War II technique of recognizing a wireless operator by his *fist*—the way he sent Morse code [523].

Radio direction finding (RDF) is also critical. In the old days, this involved triangulating the signal of interest using directional antennas at two monitoring stations. Spies might have at most a few minutes to send a message home before having to move. Modern monitoring stations use *time difference of arrival* (TDOA) to locate a suspect signal rapidly, accurately, and automatically by comparing the phase of the signals received at two sites. Nowadays, anything more than a second or so of transmission can be a giveaway.

Traffic analysis—looking at the number of messages by source and destination—can also give very valuable information, not just about imminent attacks (which were signalled in World War I by a greatly increased volume of radio messages) but also about unit movements and other routine matters. However, traffic analysis really comes into its own when sifting through traffic on public networks, where its importance (both for national intelligence and police purposes) is difficult to overstate.

If you suspect Alice of espionage (or drug dealing, or whatever), you note everyone she calls and everyone who calls her. This gives you a list of dozens of suspects. You eliminate the likes of banks and doctors, who receive calls from too many people to analyze (your *whitelist*), and repeat the procedure on each remaining number. Having done this procedure recursively several times, you have a mass of thousands of contacts, which you sift for telephone numbers that appear more than once. If (say) Bob, Camilla, and Donald are Alice's contacts, with Bob and Camilla in contact with Eve, and Donald and Eve in touch with Farquhar, then all of these people are considered to be suspects. You now draw a *friendship tree*, which gives a first approximation to Alice's network, and refine it by collating it with other intelligence sources.

This is not as easy as it sounds. People can have several numbers; Bob might get a call from Alice at his work number, then call Eve from a phone booth. (In fact, if you're running an IRA cell, your signals officer should get a job at a dentist's or a doctor's or some other place that will be called by so many different people that they will probably be whitelisted. But that's another story.) Also, you will need some means of correlating telephone numbers to people. Even if you have access to the phone company's database of unlisted numbers, prepaid mobile phones can be a serious headache, as can cloned phones and hacked PBXs. I'll discuss these in the chapter on telecomms security; for now, I'll just remark that anonymous phones aren't new. There have been public phone booths for generations. But they are not a universal answer for the crook, as the discipline needed to use them properly is beyond most criminals, and in any case causes severe disruption.

Signals collection is not restricted to agreements with phone companies for access to the content of phone calls and the communications data. It also involves a wide range of specialized facilities ranging from expensive fixed installations, which copy international satellite links, through temporary tactical arrangements. A book by Nicky Hager [368] describes the main fixed collection network operated by the United States, Canada, Britain, Australia, and New Zealand. Known as *Echelon*, this consists of a number of collection stations that monitor international phone, fax, and data traffic using computers called *dictionaries.* These search the passing traffic for interesting phone numbers, network addresses, and machine-readable content; this is driven by search strings entered by intelligence analysts. The fixed network is supplemented by tactical collection facilities as needed; Hager describes, for example, the dispatch of Australian and New Zealand navy frigates to monitor domestic communications in Fiji during military coups in the 1980s. Egmont Koch and Jochen Sperber discuss U.S. and

German installations in Germany in [464]; David Fulghum describes airborne signals collection in [324]; satellites are also used to collect signals, and there are covert collection facilities that are not known to the host country.

Despite this huge capital investment, the most difficult and expensive part of the whole operation is traffic selection, not collection [490]. Thus, contrary to naïve expectations, cryptography can make communications more vulnerable rather than less (if used incompetently, as it usually is). If you just encipher all the traffic you consider to be important, you have thereby marked it for collection by the enemy. On the other hand, if everyone encrypted all their traffic, then hiding traffic could be much easier (hence the push by signals intelligence agencies to prevent the widespread use of cryptography, even if it's freely available to individuals). This brings us to the topic of attacks.

16.3.2 Attacks on Communications

Once you have mapped the enemy network, you may wish to attack it. People often talk in terms of "codebreaking," but this is a gross oversimplification.

First, although some systems have been broken by pure cryptanalysis, this is fairly rare. Most production attacks have involved theft of key material as when the U.S. State Department code book was stolen during World War II by the valet of the U.S. ambassador to Rome or errors in the manufacture and distribution of key material as in the U.S. "Venona" attacks on Soviet diplomatic traffic [428]. Even where attacks based on cryptanalysis have been possible, they have often been made much easier by errors such as these, an example being the U.K./U.S. attacks on the German Enigma traffic during World War II [429]. The pattern continues to this day. A recent history of Soviet intelligence during the Cold War reveals that the technological advantage of the United States was largely nullified by Soviet skills in "using Humint in Sigint support"—which largely consisted of recruiting traitors who sold key material, such as the Walker family [51].

Second, access to content is often not the desired result. In tactical situations, the goal is often to detect and destroy nodes, or to jam the traffic. Jamming can involve not just noise insertion but active deception. In World War II, the Allies used German speakers as bogus controllers to send German nightfighters confusing instructions, and there was a battle of wits as authentication techniques were invented and defeated. More recently, as I noted in the chapter on biometrics, the U.S. Air Force has deployed more sophisticated systems based on voice morphing. I mentioned in an earlier chapter the tension between intelligence and operational units: the former want to listen to the other side's traffic, and the latter to deny them its use [63]. Compromises between these goals can be hard to find. It's not enough to jam the traffic you can't read, as that tells the enemy what you can read!

Matters can, in fact, be simplified if the opponent uses cryptography—even in a competent way. This removes the ops/intel tension, and you switch to RDF or link destruction as appropriate. This can involve the hard-kill approach of digging up cables or bombing telephone exchanges (both of which the allies did during the Gulf War), the soft-kill approach of jamming, or whatever combination of the two is economic. Jamming is a useful expedient where a link is to be disrupted for a short period, but is often expensive; not only does it tie up facilities, but the jammer itself becomes a target. (There are cases where it is more effective, such as against some satellite links where the uplink can be jammed using a tight beam from a hidden location using only a modest amount of power.)

The increasing use of civilian infrastructure, and in particular the Internet, raises the question of whether systematic denial-of-service attacks might be used to jam traffic. (There are anecdotes of Serbian information warfare cells attempting such attacks on NATO Web sites.) This threat is still considered real enough that many Western countries have separate intranets for government and military use.

16.3.3 Protection Techniques

As should be clear from the above, communications security techniques involve not just protecting the authenticity and confidentiality of the content—which can be achieved in a relatively straightforward way by encryption and authentication protocols—but also preventing traffic analysis, direction finding, jamming and physical destruction. Encryption can stretch to the first of these if applied at the link layer, so that all links appear to have a pseudorandom bitstream on them at all times, regardless of whether there is any message traffic. But link-layer encryption alone is not in general enough, as enemy capture of a single node might put the whole network at risk.

Encryption alone cannot protect against interception, RDF, jamming, and the destruction of links or nodes. For this, different technologies are needed. The obvious solutions are:

- Dedicated lines or optical fibers.
- Highly directional transmission links, such as optical links using infrared lasers or microwave links using highly directional antennas and extremely high frequencies, 20 GHz and up.
- *Low-probability-of-intercept* (LPI), *low-probability-of-position-fix* (LPPF), and antijam radio techniques.

The first two of these options are fairly straightforward to understand, and where feasible, they are usually the best. Cabled networks are very hard to destroy completely, unless the enemy knows where the cables are and has physical access to cut them. Even with massive artillery bombardment, the telephone network in Stalingrad remained in use (by both sides) all through the siege.

The third option is a substantial subject in itself, which I will now describe (albeit only briefly).

There are a number of LPI/LPPF/antijam techniques that go under the generic name of *spread spectrum* communications. They include *frequency hoppers, direct sequence spread spectrum* (DSSS), and *burst transmission.* From beginnings around World War II, spread-spectrum has spawned a substantial industry, and the technology (especially DSSS) has been applied to numerous other problems, ranging from high-resolution ranging (in the GPS system) through copyright marks in digital images (which I'll discuss later). Let's look at each of these three approaches in turn.

16.3.3.1 Frequency Hopping

Frequency hoppers are the simplest spread-spectrum systems to understand and to implement. They do exactly as their name suggests: they hop rapidly from one frequency to another, with the sequence of frequencies determined by a pseudorandom sequence known to the authorized principals. Hoppers were invented, famously, over dinner in 1940 by actress Hedy Lamarr and screenwriter George Antheil, who devised the technique as a means of controlling torpedos without the enemy detecting them or jamming their transmissions [484]. A frequency-hopping radar was independently developed at about the same time by the Germans [686]; in response to steady improvements in British jamming, German technicians adapted their equipment to change frequency daily, then hourly, and finally, every few seconds [627].

Hoppers are resistant to jamming by an opponent who doesn't know the hop sequence. Such an opponent may have to jam much of the band, and thus needs much more power than would otherwise be necessary. The ratio of the input signal's bandwidth to that of the transmitted signal is called the *process gain* of the system; thus, a 100 bit/sec signal spread over 10 MHz has a process gain of $10^7/10^2 = 10^5 = 50$ dB. The *jamming margin*, which is defined as the maximum tolerable ratio of jamming power to signal power, is essentially the process gain modulo implementation and other losses (strictly speaking, process gain divided by the minimum bit energy-to-noise density ratio). The optimal jamming strategy, for an opponent who can't predict the hop sequence, is *partial band jamming*—to jam enough of the band to introduce an unacceptable error rate in the signal.

Although hoppers can give a large jamming margin, they give little protection against an opponent who merely wants to detect their existence. A signal analysis receiver that sweeps across the frequency band of interest will often intercept them. (Depending on the relevant bandwidths, sweep rate, and dwell time, it might intercept a hopping signal several times).

However, because frequency hoppers are simple to implement, they are often used in combat networks, such as man-pack radios, with slow hop rates of 50–500 per second. To disrupt their communications, the enemy will need a fast or powerful jammer, which is inconvenient for the battlefield. Fast hoppers (defined in theory as having hop rates exceeding the bit rate; in practice, with hop rates of 10,000 per second or more) can pass the limit of even large jammers.

16.3.3.2 DSSS

In direct sequence spread spectrum, we multiply the information-bearing sequence by a much higher-rate pseudorandom sequence, usually generated by some kind of stream cipher. This spreads the spectrum by increasing the bandwidth (Figure 16.1). The technique was first described by a Swiss engineer, Gustav Guanella, in a 1938 patent application [686], and developed extensively in the United States in the 1950s. Its first deployment in anger was in Berlin in 1959.

Like hopping, DSSS can give substantial jamming margin (the two systems have the same theoretical performance). But it can also make the signal significantly harder to intercept. The trick is to arrange things so that at the intercept location, the signal strength is so low that it is lost in the noise floor unless you know the spreading sequence with which to recover it. Of course, it's harder to do both at the same time, since an antijam signal should be high power and an LPI/LPPF signal low power; the usual modus operandi is to work in LPI mode until detected by the enemy (for example, when coming within radar range), then boost transmitter power into antijam mode.

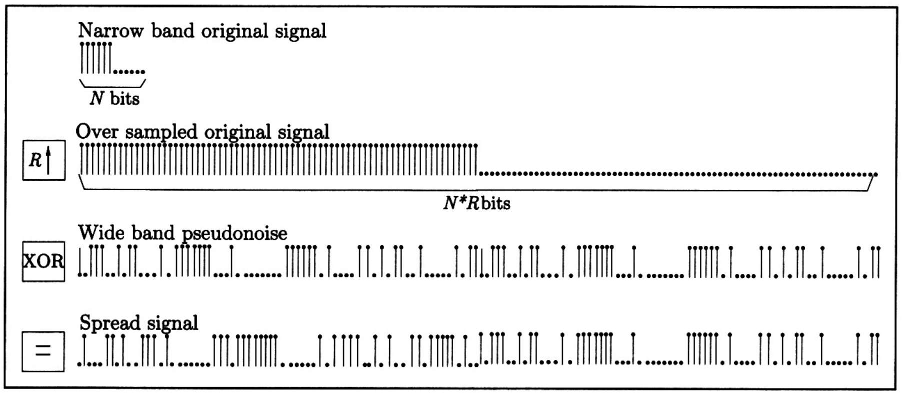

Figure 16.1 Spreading in DSSS (courtesy of Roche and Dugelay).

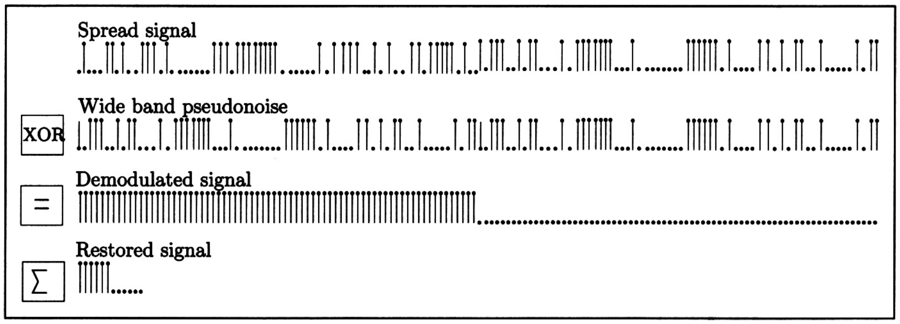

Figure 16.2 Unspreading in DSSS (courtesy of Roche and Dugelay).

There is a large literature on DSSS; and the techniques have now been taken up by the commercial world as *code division multiple access* (CDMA) in various mobile radio and phone systems. DSSS is sometimes referred to as "encrypting the RF," and it comes in a number of variants. For example, when the underlying modulation scheme is FM rather than AM, it's called *chirp*. (The classic introduction to the underlying mathematics and technology is [616].) The engineering complexity is higher than with frequency hop, for various reasons. For example, synchronization is particularly critical. Users with access to a reference time signal (such as GPS or an atomic clock) can do this much more easily; of course, if you don't control GPS, you may be open to synchronization attacks; and even if you do, the GPS signal might be jammed. (It has recently been reported that the French jammed GPS in Greece in an attempt to sabotage a British bid to sell 250 tanks to the Greek government, a deal in which France was a competitor. This caused the British tanks to get lost during trials. When the ruse was discovered, the Greeks found it all rather amusing [757].) Another strategy is to have your users take turns at providing a reference signal.

16.3.3.3 Burst Communications

Burst communications, as their name suggests, involve compressing the data and transmitting it in short bursts at times unpredictable by the enemy. They are also known as *time-hop.* Usually, they are not so jam-resistant (except insofar as the higher data rate spreads the spectrum), but they can be difficult to intercept; if the duty cycle is low, a sweep receiver can easily miss them. They are often used in radios for special forces and intelligence agents.

An interesting variant is *meteor burst* transmission (also known as *meteor scatter*). This relies on the billions of micrometeorites that strike the Earth's atmosphere each day, each leaving a long ionization trail that persists for about a third of a second, and providing a temporary transmission path between a "mother station" and an area that might be a hundred miles long and a few miles wide. The mother station transmits continuously, and whenever one of the "daughters" hears mother, it starts to send packets of data at high speed, to which mother replies. With the low power levels used in covert operations, it is possible to achieve an average data rate of about 50 bps, with an average latency of about 5 minutes and a range of 500–1,500 miles. With higher power levels, and in higher latitudes, average data rates can rise into the tens of kilobits per second.

As well as special forces, the U.S. Air Force in Alaska uses meteor scatter as backup communications for early warning radars. It's also used in civilian applications such as monitoring rainfall in Lesotho, Africa. In niche markets, where low bit rates and high latency can be tolerated, but where equipment size and cost are important, meteor scatter can be hard to beat. (The technology is described in [676].)

16.3.3.4 Combining Covertness and Jam Resistance

There are some rather complex trade-offs between different LPI, LPPF, and jam resistance technologies, and other aspects of performance such as their resistance to fading and multipath, and the number of users that can be accommodated simultaneously. They also behave differently in the face of specialized jamming techniques such as *swept-frequency jamming* (where the jammer sweeps repeatedly through the target frequency band) and *repeater jamming* (where the jammer follows a hopper as closely as it can). Some types of jamming translate; for example, an opponent with insufficient power to block a signal completely can do *partial time jamming* on DSSS by emitting pulses that cover most of its utilized spectrum, and on frequency hop by partial band jamming.

There are also engineering trade-offs. For example, DSSS tends to be about twice as efficient as frequency hop in power terms, but frequency hop gives much more jamming margin for a given complexity of equipment. On the other hand, DSSS signals are much harder to locate using direction-finding techniques [287].

System survivability requirements can impose further constraints. It may be essential to prevent an opponent who has captured one radio and extracted its current key material from using this to jam a whole network.

A typical modern military system will use some combination of tight beams, DSSS, hopping and burst.

- The Jaguar tactical radio used by U.K. armed forces hops over one of nine 6.4 MHz bands, and has an antenna with a steerable null that can be pointed at a jammer or at a hostile intercept station.
- Both DSSS and hopping are used with *Time Division Multiple Access* (TDMA) in the *Joint Tactical Information Distribution System* (JTIDS), a U.S. data link system used by AWACS—the Airborne Warning and Control System—to communicate with fighters [677]. TDMA separates transmission from reception, and lets users know when to expect their slot. The DSSS signal has a 57.6 KHz data rate and a 10 MHz chip rate (and so a jamming margin of 36.5 dB), which hops around in a 255 MHz band with a minimum jump of 30 MHz. The hopping code is available to all users, while the spreading code is limited to individual circuits. The rationale is that if an equipment capture leads to the compromise of the spreading code, this would allow jamming of only a single 10 MHz band, not the full 255 MHz.
- MILSTAR is a U.S. satellite communications system with 1-degree beams from a geostationary orbit (20 GHz down, 44 GHz up). The effect of the narrow beam is that users can operate within three miles of the enemy without being detected. Jam protection is from hopping; its channels hop several thousand times a second in bands of 2 GHz.
- A system designed to control MX missiles (but not in the end deployed) is described in [337] and gives an example of extreme survivability engineering. To be able to withstand a nuclear first strike, the system had to withstand significant levels of node destruction, jamming, and atmospheric noise. The design adopted was a frequency hopper at 450 KHz with a dynamically reconfigurable network.
- French tactical radios have remote controls. The soldier can use the handset a hundred meters from the radio. This means that attacks on the high-power emitter don't endanger the troops so much [216].

There are also some system-level tricks, such as *interference cancellation*, where the idea is to communicate in a band you are jamming and whose jamming waveform is known to your own radios, so they can cancel it out or hop around it. This can make jamming harder for the enemy by forcing him to spread his available power over a larger bandwidth, and can make signals intelligence harder, too [644].

16.3.4 Interaction Between Civil and Military Uses

Civil and military uses of communications are increasingly intertwined. Operation Desert Storm (the Gulf War against Iraq) made extensive use of the Gulf States' civilian infrastructure: a huge tactical communications network was created in a short space of time using satellites, radio links, and leased lines. Experts from various U.S. armed services claim that the effect of communications capability on the war was absolutely decisive [398]. It appears inevitable that both military and substate groups will attack civilian infrastructure to deny it to their opponents. Already, satellite links are particularly vulnerable to uplink jamming. Satellite-based systems such as GPS have been jammed as an exercise; and there is some discussion of the systemic vulnerabilities that result from overreliance on it [310].

Another example of growing interdependency is given by the Global Positioning System, GPS. This started as a U.S. military navigation system, and had a *selective availability* feature that limited the accuracy to about a hundred yards unless the user had the relevant cryptographic key. This had to be turned off during Desert Storm as there weren't enough military GPS sets to go around, and civilian equipment had to be used instead. As time went on, GPS turned out to be so useful, particularly in civil aviation, that the FAA helped find ways to defeat selective availability that give an accuracy of about three yards, compared with a claimed eight yards for the standard military receiver [270]. Finally, in May 2000, President Clinton announced the cessation of selective availability. (Presumably, this preserves its usability in wartime.)

The civilian infrastructure also provides some defensive systems of which government organizations (especially in the intelligence field) can make use. I mentioned the prepaid mobile phone, which provides a fair degree of anonymity; secure Web servers offer some possibilities; and another example is the *anonymous remailer*, a device that accepts encrypted email, decrypts it, and sends it on to a destination contained within the outer encrypted envelope. I'll discuss this technology in more detail in Section 20.4.3; one of the pioneers of anonymous networking was the U.S. Navy [637]. Conspiracy theorists suspect that public use of the system provides cover traffic for classified messages.

Although communications security on the Net has, until now, been interpreted largely in terms of message confidentiality and authentication, it looks likely that the future will become much more like military communications, in that various kinds of service denial attacks, anonymity, and deception plays will become increasingly important. I'll return to this theme later. For now, let's look at the aspects of electronic warfare that have to do with target acquisition and weapon guidance, as these are where the arts of jamming and deception have been most highly developed. (In fact, although there is much more in the open literature on the application of electronic attack and defense to radar than to communications, much of the same material clearly applies to both.)

16.4 Surveillance and Target Acquisition

Although some sensor systems use passive direction finding, the main methods used to detect hostile targets and guide weapons to them are sonar, radar, and infrared. The first of these to be developed was sonar, which was invented and deployed in World War I (under the name of Asdic) [366]. Except in submarine warfare, the key sensor is radar. Although radar was invented by Christian Hülsmeyer in 1904 as a maritime anticollision device, its serious development only occurred in the 1930s, and it was used by all major participants in World War II [369, 424]. The electronic attack and protection techniques developed for it tend to be better developed than, and often go over to, systems using other sensors. In the context of radar, "electronic attack" usually means jamming (though in theory it also includes stealth technology), and "electronic protection" refers to the techniques used to preserve at least some radar capability.

16.4.1 Types of Radar

A very wide range of systems are in use, including search radars, fire-control radars, terrain-following radars, counterbombardment radars, and weather radars. They have a wide variety of signal characteristics. For example, radars with a low RF and a low *pulse repetition frequency* (PRF) are better for search, while high-frequency, high PRF devices are better for tracking. A good textbook on the technology is by Schleher [677].

Simple radar designs for search applications may have a rotating antenna that emits a sequence of pulses and detects echos. This was an easy way to implement radar in the days before digital electronics; the sweep in the display tube could be mechanically rotated in synch with the antenna. Fire-control radars often used *conical scan;* the beam would be tracked in a circle around the target's position, and the amplitude of the returns could drive positioning servos (and weapon controls) directly. Now the beams are often generated electronically using multiple antenna elements, but tracking loops remain central. Many radars have a *range gate*, circuitry that focuses on targets within a certain range of distances from the antenna; if the radar had to track all objects between, say, 0 and 100 miles, then its pulse repetition frequency would be limited by the time it takes radio waves to travel 200 miles. This would have consequences for angular resolution and for tracking performance generally.

Doppler radar measures the velocity of the target by the change in frequency in the return signal. It is very important in distinguishing moving targets from *clutter*, the returns reflected from the ground. Doppler radars may have *velocity gates* that restrict attention to targets whose radial speed with respect to the antenna is within certain limits.

16.4.2 Jamming Techniques

Electronic attack techniques can be passive or active.

The earliest countermeasure to be widely used was *chaff*—thin strips of conducting foil cut to a half the wavelength of the target signal, then dispersed to provide a false return. Toward the end of World War II, allied aircraft were dropping 2,000 tons of chaff a day to degrade German air defenses. Chaff can be dropped directly by the aircraft attempting to penetrate the defenses (which isn't ideal, as they will then be at the apex of an elongated signal) or by support aircraft, or fired forward into a suitable pattern using rockets or shells. The main counter-countermeasure against chaff is the use of Doppler radars; the chaff is very light, so it comes to rest almost at once and can be distinguished fairly easily from moving targets.

Other techniques include small decoys with active repeaters that retransmit radar signals, and larger decoys that simply reflect them; sometimes one vehicle (such as a helicopter) acts as a decoy for another more valuable one (such as an aircraft carrier). The principles are quite general. Weapons that home using RDF are decoyed by special drones that emit seduction RF signals, while infrared guided missiles are diverted using flares.

The passive countermeasure in which the most money has been invested is *stealth*, reducing the *radar cross-section* (RCS) of a vehicle so that it can be detected only at very much shorter range. This means, for example, that the enemy has to place his air defense radars closer together, so he has to buy a lot more of them. Stealth includes a wide range of techniques, and a proper discussion is well beyond the scope of this book. Some people think of it as "extremely expensive black paint," but there's more to it than that. Because an aircraft's RCS is typically a function of its aspect, it may have a fly-by-wire system that continually exhibits an aspect with a low RCS to identified hostile emitters.

Active countermeasures are much more diverse. Early jammers simply generated a lot of noise in the range of frequencies used by the target radar; this technique is known as *noise jamming* or *barrage jamming.* Some systems used systematic frequency patterns, such as pulse jammers, or swept jammers which traversed the frequency range of interest (also known as *squidging oscillators*). But such a signal is fairly easy to block—one trick is to use a *guard band* receiver, a receiver on a frequency adjacent to the one in use, and to blank the signal when this receiver shows a jamming signal. It should also be noted that jamming isn't restricted to one side. As well as being used by the radar's opponent, the radar itself can also send suitable spurious signals from an auxiliary antenna to mask the real signal or simply to overload the defenses.

At the other end of the scale lie hard-kill techniques such as *anti-radiation missiles* (ARMs), often fired by support aircraft, which home in on the sources of hostile signals. Defenses against such weapons include the use of decoy transmitters, and blinking transmitters on and off.

In the middle lies a large toolkit of *deception jamming* techniques. Most jammers used for self-protection are deception jammers of one kind or another; barrage and ARM techniques tend to be more suited to use by support vehicles.

The usual goal with a self-protection jammer is to deny range and bearing information to attackers. The basic trick is *inverse gain jamming* or *inverse gain amplitude modulation.* This is based on the observation that the directionality of the attacker's antenna is usually not perfect; in addition to the main beam, it has *sidelobes* through which energy is also transmitted and received, albeit much less efficiently. The sidelobe response can be mapped by observing the transmitted signal, and a jamming signal can be generated so that the net emission is the inverse of the antenna's directional response. The effect, as far as the attacker's radar is concerned, is that the signal seems to come from everywhere; instead of a "blip" on the radar screen you see a circle centered on your own antenna. Inverse gain jamming is very effective against the older conical-scan fire-control systems.

More generally, the technique is to retransmit the radar signal with a systematic change in delay and/or frequency. This can be either noncoherent, in which case the jammer is called a *transponder*, or coherent—that is, with the right waveform—when it's a *repeater.* (It is now common to store received waveforms in *digital radio frequency memory* (DRFM) and manipulate them using signal processing chips.)

An elementary countermeasure is *burn-through.* By lowering the pulse repetition frequency, the dwell time is increased, so the return signal is stronger—at the cost of less precision. A more sophisticated countermeasure is *range gate pull-off* (RGPO). Here, the jammer transmits a number of fake pulses that are stronger than the real ones, thus capturing the receiver, and then moving them out of phase so that the target is no longer in the receiver's range gate. Similarly, with Doppler radars the basic trick is *velocity gate pull-off* (VGPO). With older radars, successful RGPO would cause the radar to break lock and the target to disappear from the screen. Modern radars can reacquire lock very quickly, so RGPO must either be performed repeatedly or combined with another technique—commonly, with inverse gain jamming to break angle tracking at the same time.

An elementary counter-countermeasure is to jitter the pulse repetition frequency. Each outgoing pulse is either delayed or not, depending on a *lag sequence* generated by a stream cipher or random number generator. This means that the jammer cannot anticipate when the next pulse will arrive, and so has to follow it. Such *follower jamming* can only make false targets that appear to be further away. The (counter)^3-measure is for the radar to have a *leading-edge tracker*, which responds only to the first return pulse; and the (counter)^4-measures can include jamming at such a high power that the receiver's automatic gain control circuit is captured, or *cover jamming* in which the jamming pulse is long enough to cover the maximum jitter period.

The next twist of the screw may involve tactics. Chaff is often used to force a radar into Doppler mode, which makes PRF jitter difficult (as continuous waveforms are better than pulsed for Doppler), while leading-edge trackers may be combined with frequency agility and smart signal processing. For example, true target returns fluctuate, and have realistic accelerations, while simple transponders and repeaters give out a more or less steady signal. Of course, it's always possible for designers to be too clever; the Mig-29 could decelerate more rapidly in level flight by a rapid pull-up than some radar designers had anticipated, and so pilots could use this maneuver to break radar lock. And now, of course, enough MIPS are available to manufacture realistic false returns.

16.4.3 Advanced Radars and Countermeasures

A number of advanced techniques are used to give an edge on the jammer.

Pulse compression, first developed in Germany in World War II, uses a kind of direct sequence spread-spectrum pulse, filtered on return by a matched filter to compress it again. This can give processing gains of 10–1,000. Pulse compression radars are resistant to transponder jammers, but are vulnerable to repeater jammers, especially those with digital radio frequency memory. However, the use of LPI waveforms is important if you do not wish the target to detect you first.

Pulsed Doppler is much the same as Doppler, and sends a series of phase stable pulses. It has come to dominate many high-end markets, and is widely used, for example, in *look-down shoot-down* systems for air defense against low-flying intruders. As with elementary pulsed tracking radars, different RF and pulse repetition frequencies have different characteristics: we want low-frequency/PRF for unambiguous range/velocity and also to reduce clutter—but this can leave many blind spots. Airborne radars that have to deal with many threats use high PRF and look only for velocities above some threshold, say 100 knots—but are weak in tail chases. The usual compromise is medium PRF—but this suffers from severe range ambiguities in airborne operations. Also, search radar requires long, diverse bursts, whereas tracking needs only short, tuned ones. An advantage is that pulsed Doppler can discriminate some very specific signals, such as modulation provided by turbine blades in jet engines. The main deception strategy used against pulsed Doppler is velocity gate pull-off, although a new variant is to excite multiple velocity gates with deceptive returns.

Monopulse is becoming one of the most popular techniques. It is used, for example, in the Exocet missiles that proved so difficult to jam in the Falklands war. The idea is to have four linked antennas so that azimuth and elevation data can be computed from each return pulse using interferometric techniques. Monopulse radars are difficult and expensive to jam, unless a design defect can be exploited; the usual techniques involve tricks such as formation jamming and terrain bounce. Often the preferred defensive strategy is just to use towed decoys.

One of the more recent tricks is *passive coherent location*. Lockheed's Silent Sentry system has no emitters at all, but rather utilizes reflections of commercial radio and television broadcast signals to detect and track airborne objects [508]. The receivers, being passive, are hard to locate and attack; and knocking out the system entails destroying major civilian infrastructures, which opponents will often prefer not to do for various propaganda reasons. This strategy is moderately effective against some kinds of stealth technology.

The emergence of digital radio frequency memory and other software radio techniques holds out the prospect of much more complex attack and defense. Both radar and jammer waveforms may be adapted to the tactical situation with much greater flexibility than before. But fancy combinations of spectral, temporal, and spatial characteristics will not be the whole story. Effective electronic attack is likely to continue to require the effective coordination of different passive and active tools with weapons and tactics. The importance of intelligence, and of careful deception planning, is likely to increase.

16.4.4 Other Sensors and Multisensor Issues

Much of what I've said about radar applies to sonar as well, and a fair amount applies to infrared. Passive decoys—flares—worked very well against early heat-seeking missiles that used a mechanically spun detector, but are less effective against modern detectors that incorporate signal processing. Flares are like chaff in that they decelerate rapidly with respect to the target, so the attacker can filter on velocity or acceleration. Flares are also like repeater jammers in that their signals are relatively stable and strong compared with real targets.

Active infrared jamming is harder, and thus less widespread, than radar jamming. It tends to exploit features of the hostile sensor by pulsing at a rate or in a pattern that causes confusion. Some infrared defense systems are starting to employ lasers to disable the sensors of incoming weapons; and it has recently been admitted that a number of UFO sightings were actually due to various kinds of jamming (both radar and infrared) [75].

One growth area is *multisensor data fusion*, whereby inputs from radars, infrared sensors, video cameras, and even humans are combined to give better target identification and tracking than any could individually. The Rapier air defense missile, for example, uses radar to acquire azimuth while tracking is carried out optically in visual conditions. Data fusion can be harder than it seems. As discussed in Section 13.8, combining two alarm systems will generally result in improving either the false alarm or the missed alarm rate, while making the other worse. If you scramble your fighters when you see a blip on either the radar or the infrared, there will be more false alarms;

but if you scramble only when you see both, it will be easier for the enemy to jam you or to sneak through.

System issues become more complex where the attacker himself is on a platform that's vulnerable to counterattack, such as a fighter bomber. He will have systems for threat recognition, direction finding, and missile approach warning; and the receivers in these will be deafened by his jammer. The usual trick is to turn the jammer off for a short "look-through" period at random times.

With multiple friendly and hostile platforms, things get much more complex still. Each side might have specialist support vehicles with high-power dedicated equipment, which makes it to some extent an energy battle—"he with the most watts wins." A SAM belt may have multiple radars at different frequencies to make jamming harder. The overall effect of jamming (as of stealth) is to reduce the effective range of radar. But the jamming margin also matters, and who has the most vehicles, and the tactics employed.

With multiple vehicles engaged, it's also necessary to have a reliable way of distinguishing friend from foe.

16.5 IFF Systems

The technological innovations of World War II—and especially jet aircraft, radar, and missiles—made it impractical to identify targets visually, and imperative to have an automatic way to *identify friend or foe* (IFF). Early IFF systems emerged during that war, using a vehicle serial number or "code of the day"; but this is open to spoofing. Since the 1960s, U.S. aircraft have used the Mark XII system, which has cryptographic protection as discussed in Section 2.3. Here, it isn't the cryptography that's the hard part, but rather the protocol and operational problems.

The Mark XII has four modes, of which the secure mode uses a 32-bit challenge and a 4-bit response. This is a precedent set by its predecessor, the Mark X; if challenges or responses were too long, the radar's pulse repetition frequency (and thus it accuracy) would be degraded. The Mark XII sends a series of 12–20 challenges at a rate of one every four milliseconds. In the original implementation, the responses were displayed on a screen at a position offset by the arithmetic difference between the actual response and the expected one. The effect was that while a foe had a null or random response, a friend would have responses at or near the center screen, which would light up. Reflection attacks are prevented, and MIG-in-the-middle attacks made much harder, because the challenge uses a focused antenna, while the receiver is omnidirectional. (In fact, the antenna used for the challenge is typically the fire control radar, which in older systems was conically scanned).

I mentioned in Section 2.3 that cryptographic protection alone isn't bulletproof: the enemy might record and replay valid challenges, with a view to using your IFF signal for direction finding purposes. This can be a real problem in dense operational areas with many vehicles and emitters, such as on the border between East and West Germany during the Cold War, and parts of the Middle East to this day. There, the return signal can be degraded by overlapping signals from nearby aircraft—an effect known as *garbling*. In the other direction, aircraft transponders subjected to many challenges may be unable to decode them properly—an effect known as *fruiting*. Controlling these phenomena means minimizing the length of challenge and response signals, which limits the usefulness of cryptographic protection. As a result, the Royal Air Force resisted American demands to make the Mark XII a NATO requirement and continues using the World-War-II-vintage Mark X, changing the codes every 30 minutes. (The details of Mark X and Mark XII, and the R.A.F.-U.S.A.F. debate, can be found in [348].) This is yet another example of the surprising difficulty of getting cryptography to add value to a system design.

The system-level issues are even less tractable. The requirement is to identify enemy forces, but an IFF system reliant on cooperation from the target can only identify friends positively. Neither neutrals, nor friends with defective or incorrectly set transponders, can be distinguished from enemies. So while IFF may be used as a primary mechanism in areas where neutrals are excluded (such as in the vicinity of naval task forces at sea in wartime), its more usual use is as an adjunct to more traditional methods, such as correlation with flight plans. In this role it can still be very valuable.

Since the Gulf war, in which 25% of Allied troop casualties were caused by "friendly fire", a number of experimental systems have been developed that extend IFF to ground troops. One U.S. system combines laser and RF components. Shooters have lasers, and soldiers have transponders; when the soldier is illuminated with a suitable challenge, his equipment broadcasts a "don't shoot me" message using frequency-hopping radio [820]. An extension allows aircraft to broadcast targeting intentions on millimeter wave radio. This system was due to be fielded in the year 2000. Britain is developing a cheaper system called MAGPIE, in which friendly vehicles carry a low-probability-of-intercept millimeter wave transmitter, and shooters carry a directional receiver [381]. (Dismounted British foot soldiers, unlike their American counterparts, have no protection.) Other countries are developing yet other systems.

16.6 Directed Energy Weapons

In the late 1930s, there was panic in Britain and America on rumors that the Nazis had developed a high-power radio beam that would burn out vehicle ignition systems. British scientists studied the problem and concluded that this was infeasible [424]. They were correct—given the relatively low-powered radio transmitters, and the simple but robust vehicle electronics, of the 1930s.

Things started to change with the arrival of the atomic bomb. The detonation of a nuclear device creates a large pulse of gamma-ray photons, which in turn displace electrons from air molecules by *Compton scattering*. The large induced currents give rise to an *electromagnetic pulse* (EMP), which may be thought of as a very high amplitude pulse of radio waves with a very short rise time.

Where a nuclear explosion occurs within the earth's atmosphere, the EMP energy is predominantly in the VHF and UHF bands, though there is enough energy at lower frequencies for a *radio flash* to be observable thousands of miles away. Within a few tens of miles of the explosion, the radio frequency energy may induce currents large enough to damage most electronic equipment that has not been hardened. The effects of a blast outside the earth's atmosphere are believed to be much worse (although there has never been a test). The gamma photons can travel thousands of miles before they strike the earth's atmosphere, which could ionize to form an antenna on a continental scale. It is reckoned that most electronic equipment in Northern Europe could be burned out by a one megaton blast at a height of 250 miles above the North Sea. For this reason, critical military systems are carefully shielded.

Western concern about EMP grew after the Soviet Union started a research program on non-nuclear EMP weapons in the mid-80s. At the time, the United States was deploying "neutron bombs" in Europe—enhanced radiation weapons that could kill people without demolishing buildings. The Soviets portrayed this as a "capitalist bomb" which would destroy people while leaving property intact, and responded by threatening a "socialist bomb" to destroy property (in the form of electronics) while leaving the surrounding people intact.

By the end of World War II, the invention of the cavity magnetron had made it possible to build radars powerful enough to damage unprotected electronic circuitry for a range of several hundred yards. The move from valves to transistors and integrated circuits has increased the vulnerability of most commercial electronic equipment. A terrorist group could in theory mount a radar in a truck and drive around a city's financial sector wiping out the banks. For battlefield use, a more compact form factor is preferred, and so the Soviets are said to have built high-energy RF (HERF) devices from capacitors, magnetohydrodynamic generators and the like.

By the mid 1990s, the concern that terrorists might get hold of these weapons from the former Soviet Union led the agencies to try to sell commerce and industry on the idea of electromagnetic shielding. These efforts were dismissed as hype. Personally, I tend to agree. The details of the Soviet HERF bombs haven't been released, but physics suggests that EMP is limited by the dielectric strength of air and the cross-section of the antenna. In nuclear EMP, the effective antenna size could be a few hundred meters for an endoatmospheric blast, up to several thousand kilometers for an exoatmospheric one. But in "ordinary" EMP/HERF, it seems that the antenna will be at most a few meters. NATO planners concluded that military command and control systems that were already hardened for nuclear EMP should be unaffected.

As for the civilian infrastructure, I suspect that a terrorist can do a lot more damage with an old-fashioned truck bomb made with a ton of fertilizer and fuel oil, and he doesn't need a PhD in physics to design one! Anyway, the standard reference on EMP is [645].

Concern remains however, that the EMP from a single nuclear explosion 250 miles above the central United States could do colossal economic damage, while killing few people directly [53]. This potentially gives a blackmail weapon to countries such as Iran and North Korea, both of which have nuclear ambitions but primitive infrastructures. In general, a massive attack on electronic communications is more of a threat to countries such as the United States that depend heavily on them than on countries such as North Korea, or even China, that don't. This observation goes across to attacks on the Internet as well, so let's now turn to information warfare.

16.7 Information Warfare

Since about 1995, the phrase *information warfare* has come into wide use. Its popularity appears to have been catalyzed by operational experience in Desert Storm. There, air power was used to degrade the Iraqi defenses before the land attack was launched; and one goal of NSA personnel supporting the allies was to enable the initial attack to be made without casualties—even though the Iraqi air defenses were at that time intact and alert. The attack involved a mixture of standard e-war techniques, such as jammers and antiradiation missiles; cruise missile attacks on command centers; attacks by special forces, who sneaked into Iraq and dug up lengths of communications cabling from the desert; and, allegedly, the use of hacking tricks to disable computers and telephone exchanges. (By 1990, the U.S. Army was already calling for bids for virus production [518].) The operation successfully achieved its mission of ensuring zero Allied casualties on the first night of the aerial bombardment. Military planners and think tanks started to consider how the success could be extended.

There is little agreement about definitions. The conventional view, arising out of Desert Storm, was expressed by Major YuLin Whitehead ([790, p 9]):

> *The strategist . . . should employ [the information weapon] as a precursor weapon to blind the enemy prior to conventional attacks and operations.*

The more aggressive view is that properly conducted information operations should encompass everything from signals intelligence to propaganda; and, given the reliance that modern societies place on information, it should suffice to break the enemy's will without fighting.

16.7.1 Definitions

In fact, there are roughly three views on what information warfare means:

- It is just a remarketing of the stuff that the agencies have been doing for decades anyway, in an attempt to maintain the agencies' budgets post-Cold-War.
- It consists of the use of hacking in a broad sense—network attack tools, computer viruses, and so on—in conflict between states or substate groups, in order to deny critical military and other services, whether for operational or propaganda purposes. It has been observed, for example, that the Internet, though designed to withstand thermonuclear bombardment, was knocked out by the Morris worm.
- It extends the electronic warfare doctrine of controlling the electromagnetic spectrum to control of all information relevant to the conflict. It thus extends traditional e-war techniques, such as radar jammers, by adding assorted hacking techniques, but also incorporates propaganda and news management.

The first of these views was the one taken by some cynical defense insiders to whom I've spoken. The second is the popular view found in newspaper articles, and also Whitehead's. It's the one I'll use as a guide in this section, but without taking a position on whether it actually contains anything really new, either technically or doctrinally.

The third finds expression in a book by Dorothy Denning [235], whose definition of information warfare is, "operations that target or exploit information media in order to win some advantage over an adversary." Its interpretation is so broad that it includes not just hacking but all of electronic warfare and all existing intelligence-gathering techniques (from sigint through satellite imagery to spies), and propaganda, too. In a later article, she's discussed the role of the Net in the propaganda and activism surrounding the Kosovo war [236]. However the bulk of her book is given over to computer security and related topics.

A similar view of information warfare, and from a writer whose background is defense planning rather than computer security, is by Edward Waltz [790]. He defines *information superiority* as "the capability to collect, process and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same". The theory is that such superiority will allow the conduct of operations without effective opposition. The book has less technical detail on computer security matters than Denning's, but sets forth a first attempt to formulate a military doctrine of information operations.

16.7.2 Doctrine

When writers such as Denning and Waltz include propaganda operations in information warfare, the cynical defense insider may remark that nothing has changed. From Roman and Mongol efforts to promote a myth of invincibility, through the use of propaganda radio stations by both sides in World War II and the Cold War, to the bombing of Serbian TV during the Kosovo campaign and denial-of-service attacks on Chechen Web sites by Russian agencies [198]—the tools may change but the game remains the same.

But there is a twist, perhaps thanks to government and military leaders' lack of familiarity with the Internet. When teenage kids deface a U.S. government department Web site, an experienced computer security professional is likely to see it as the equivalent of graffiti scrawled on the wall of a public building. After all, it's easy enough to do, and easy enough to remove. But the information warfare community can paint it as undermining the posture of information dominance that a country must project in order to deter aggression.

So there is a fair amount of debunking to be done before the political and military leadership can start to think clearly about the issues. For example, it's often stated that information warfare provides casualty-free way to win wars: "just hack the Iranian power grid and watch them sue for peace." The three obvious comments are as follows.

- The denial-of-service attacks that have so far been conducted on information systems without the use of physical force have mostly had a transient effect. A computer goes down; the operators find out what happened; they restore the system from backup and restart it. An outage of a few hours may be enough to let a wave of bombers get through unscathed, but it appears unlikely to bring a country to its knees. In this context, the failure of the Millennium Bug to cause the expected damage may be a useful warning.
- Insofar as there is a vulnerability, developed countries are more exposed. The power grid in the United States or Britain is much more computerized than that in the average developing country.
- Finally, if such an attack causes the deaths of several dozen people in Iranian hospitals, the Iranians aren't likely to see the matter much differently from a conventional military attack that killed the same number of people. Indeed, if information war targets civilians to greater extent than the alternatives, then the attackers' leaders are likely to be portrayed as war criminals. The Pinochet case, in which a former head of government only escaped extradition on health grounds, should give pause for thought.

Having made these points, I will restrict discussion in the rest of this section to technical matters.

16.7.3 Potentially Useful Lessons from Electronic Warfare

Perhaps the most important policy lesson from the world of electronic warfare is that conducting operations that involve more than one service is very much harder than it looks. Things are bad enough when army, navy, and air force units have to be coordinated—during the U.S. invasion of Grenada, a ground commander had to go to a pay phone and call home using his credit card in order to call down an air strike, as the different services' radios were incompatible. (Indeed, this was the spur for the development of software radios [482]). Things are even worse when intelligence services are involved, as they don't train with warfighters in peacetime, and so take a long time to become productive once the fighting starts. Turf fights also get in the way: under current U.S. rules, the air force can decide to bomb an enemy telephone exchange but has to get permission from the NSA and/or CIA to hack it [63]. The U.S. Army's communications strategy is now taking account of the need to communicate across the traditional command hierarchy, and to make extensive use of the existing civilian infrastructure [672].

At the technical level, many concepts may go across from electronic warfare to information protection in general.

- The electronic warfare community uses guard band receivers to detect jamming, so it can be filtered out (for example, by blanking receivers at the precise time a sweep jammer passes through their frequency). Using bait addresses to detect spam is essentially the same concept.
- There is also an analogy between virus recognition and radar signal recognition. Virus writers may make their code *polymorphic*, in that it changes its form as it propagates, to make life harder for the virus scanner vendors. Similarly, radar designers use very diverse waveforms to make it harder to store enough of the waveform in digital radio frequency memory to do coherent jamming effectively.
- Our old friends, the false accept and false reject rate, will continue to dominate tactics and strategy. As with burglar alarms or radar jamming, the ability to cause many false alarms (however crudely) will always be worth something: as soon as the false alarm rate exceeds about 15%, operator performance is degraded. As for filtering, it can usually be cheated.
- The limiting economic factor in both attack and defense will increasingly be the software cost, and the speed at which new tools can be created and deployed.
- It is useful, when subjected to jamming, not to let the jammer know whether, or how, his attack is succeeding. In military communications, it's usually better to respond to jamming by dropping the bit rate rather than by boosting power; similarly, when a nonexistent credit card number is presented at your Web site, you might say, "Sorry, bad card number, try again," but the second time it happens you should take a different line (or the attacker will keep on trying). Something such as, "Sorry, the items you have requested are tempo-

rarily out of stock and should be mailed within five working days" may do the trick.

- Although defense in depth is in general a good idea, you have to be careful of interactions between the different defenses. The classic case in e-war is when chaff dispensed by a warship to defend against an incoming cruise missile knocks out its anti-aircraft guns. The side effects of defenses can also be exploited. The most common case on the Net is the mail bomb: an attacker forges offensive newsgroup messages, which appear to come from the victim, who then gets subjected to a barrage of abuse and attacks.
- Finally, some perspective can be drawn from the differing roles of hard kill and soft kill in electronic warfare. Jamming and other soft-kill attacks can be cheaper in the short term; they can be used against multiple threats; and they have reduced political consequences. But damage assessment is hard, and you may just divert the weapon to another target. As most i-war is soft kill, these comments can be expected to go across, too.

16.7.4 Differences Between E-War and I-War

There are differences as well as similarities between traditional electronic warfare and the kinds of attack that can potentially be run over the Net.

- There are roughly two kinds of war: open war and guerilla war. Electronic warfare comes into its own in the former case, such as in air combat, most naval engagements, and the desert. In forests and mountains, the man with the AK-47 can still get a result against mechanized forces. Guerilla war has largely been ignored by the e-war community, except insofar as they make and sell radars to detect snipers and concealed mortar batteries.

  In cyberspace, the "forests and the mountains" are likely to be the large numbers of insecure hosts belonging to friendly or neutral civilians and organizations. The distributed denial-of-service (DDoS) attack, in which hundreds of innocent machines are subverted and used to bombard a target Web site with traffic, has no real analogue in the world of electronic warfare. Nevertheless, it is the likely platform for launching attacks even on "open" targets such as large commercial Web sites. So it's unclear where the open countryside in cyberspace actually is.

- Another possible source of asymmetric advantage for the guerilla is complexity. Large countries have many incompatible systems; this makes little difference when fighting another large country with similarly incompatible systems, but can leave them at a disadvantage to a small group that has built simple, coherent systems.
- Anyone trying to attack the United States is unlikely to repeat Saddam Hussein's mistake of trying to fight a tank battle. Guerilla warfare will be the norm, and cyberspace appears to be fairly well suited for this.

- There is no electronic warfare analogue of "script kiddies," people who download attack scripts and launch them without really understanding how they work. That such powerful weapons are available universally, and for free, has few analogues in meatspace. Perhaps the closest is in the lawless areas of countries such as Afghanistan, where all men go about with military weapons.

16.8 Summary

Electronic warfare is much more developed than most other areas of information security. There are many lessons to be learned, from the technical level up through the tactical level to matters of planning and strategy. We can expect that, as information warfare evolves from a fashionable concept to established doctrine, these lessons will become important for practitioners.

Research Problems

An interesting research problem is how to port techniques and experience from the world of electronic warfare to the Internet. This chapter is only a sketchy first attempt at setting down the possible parallels and differences.

Further Reading

A good (although nontechnical) introduction to radar is by P. S. Hall [369]. The best all-round reference for the technical aspects of electronic warfare, from radar through stealth to EMP weapons, is by Curtis Schleher [677]; a good summary was written by Doug Richardson [644]. The classic introduction to the anti-jam properties of spread-spectrum sequences is by Andrew Viterbi [778]; the history of spread-spectrum is ably told by Robert Scholtz [686]; the classic introduction to the mathematics of spread-spectrum is by Raymond Pickholtz, Donald Schilling, and Lawrence Milstein [616]; while the standard textbook is by Robert Dixon [254]. An overall history of British electronic warfare and scientific intelligence, which was written by a true insider, that gives a lot of insight not just into how the technology developed but also into strategic and tactical deception, is by R. V. Jones [424, 425].

Finally, the history of the technical aspects of radar, jammers, and IFF systems is available from three different and complementary viewpoints: the German by David Pritchard [627], the British by Jack Gough [348], and the American by Robert Buderi [142].