CHAPTER

19

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

19.1 Introduction

For decades, electronic warfare has been a separate subject from computer security, even though they use 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 Pentagon's embrace of information warfare as a slogan in the last years of the twentieth century established its importance — even if its concepts, theory and doctrine are still underdeveloped. The Russian denial-of-service attacks on Estonia in 2007 have put it firmly on many policy agendas — even though it's not clear that these attacks were conducted by the Russian government; as far as we know, it may have been just a bunch of Russian hackers.

There are other reasons why a knowledge of electronic warfare is important to the security engineer. Many technologies originally developed for the warrior have been adapted for commercial use, and instructive parallels abound. 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 ignored for years. It suddenly took center stage a few years ago thanks to denial-of-service attacks on commercial web sites, and when blackmailers started taking down Internet gambling sites and demanding to be paid off, it got serious.

As I develop this discussion, I'll try to draw out the parallels between electronic warfare and other information security problems. 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; and
3. exploitation, which includes not just eavesdropping but obtaining any operationally valuable information from the enemy's use of his electronic systems.

19.2 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; and
- *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 [1121]. 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*, or 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 increasingly 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 (so-called *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; a *communications* links which take sensor data to the command and control center; and output devices such as jammers, lasers, missiles, bombs 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.

19.3 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 [923]. Nowadays, a typical command and control structure is made up of various tactical and strategic radio networks supporting data, voice and images, operating 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. A significant historical threat here was that the cipher security might be penetrated and the orders, situation reports and so on compromised, whether as a result of 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 he sends messages using a medium which the enemy can monitor, such as the public telephone network or radio, then much of his 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 [506]. As voice morphing techniques are developed for commercial use, the risk of spoofing attacks on unprotected communications will increase. So cipher security may include authenticity as well as confidentiality and 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's warning receiver) but that is in tension with the power levels needed to defeat defensive jamming systems. One solution is to make the communications adaptive — to start off in a low-probability-of-intercept mode and ramp up the power if needed in response to jamming.

So 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 — which were routinely jammed by the Russians. The idea was that unless the Russians were prepared to turn off their jammers, they would have 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 sums 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 the adversary to disable the remaining third by attempting to pass all his traffic over a third of his installed capacity [789]. 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 [923].

NATO developed a comparable doctrine, called *Counter-Command, Control and Communications* operations (C-C3, pronounced C C cubed), in the 80s. It achieved its first flowering in the Gulf War. 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.

19.3.1 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 components 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*, or RFID, technology was declassified in the mid-1990s for use in identifying cloned cellular telephones, where its makers claim a 95% success rate [534, 1121]. It is the direct descendant of the World War 2 technique of recognizing a wireless operator by his *fist* — the way he used Morse Code [836].

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. So spies might have several 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; 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 1 by a greatly increased volume of

radio messages) but also about unit movements and other more 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. Until a few years ago, traffic analysis was the domain of intelligence agencies — when NSA men referred to themselves as 'hunter-gatherers', traffic analysis was much of the 'hunting'. In the last few years, however, traffic analysis has come out of the shadows and become a major subject of study.

One of the basic techniques is the *snowball search*. 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 — they accumulate like a snowball rolling downhill. You now sift the snowball you've collected — for example, for people already on one of your blacklists, and for telephone numbers that appear more than once. So if 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 may be considered 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. *Covert community detection* has become a very hot topic since 9/11, and researchers have tried all sorts of hierarchical clustering and graph partitioning methods to the problem. As of 2007, the leading algorithm is by Mark Newman [966]; it uses spectral methods to partition a network into its natural communities so as to maximise modularity.

But even given good mathematical tools for analysing abstract networks, reality is messier. People can have several numbers, and people share numbers. When conspirators take active countermeasures, it gets harder still; Bob might get a call from Alice at his work number and then call Eve from a phone box. (If you're running a terrorist cell, your signals officer should get a job at a dentist's or a doctor's or some other place that's likely to be whitelisted.) 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. Tying IP addresses to people is even harder; ISPs don't always keep the Radius logs for long. I'll discuss all these issues in more detail in later chapters; for now, I'll just remark that anonymous communications aren't new. There have been letter boxes and public phone booths for generations. But they are not a universal answer for the crook as the discipline needed to use anonymous communications properly is beyond most criminals. It's reported, for example, that the 9/11 mastermind Khalid Sheikh Mohammed

was caught after he used in his mobile phone in Pakistan a prepaid SIM card that had been bought in Switzerland in the same batch as a SIM that had been used in another Al-Qaida operation.

Signals collection is not restricted to getting phone companies to give access to the content of phone calls and the itemised billing records. It also involves a wide range of specialized facilities ranging from expensive fixed installations that copy international satellite links, down to temporary tactical arrangements. A book by Nicky Hagar [576] describes the main fixed collection network operated by the USA, Canada, the UK, Australia and New Zealand. Known as *Echelon*, this consists of a number of fixed collection stations that monitor international phone, fax and data traffic with computers called *dictionaries* which search passing traffic for interesting phone numbers, network addresses and machine-readable content; this is driven by search strings entered by intelligence analysts. One can think of this as a kind of Google for the world's phone system (though given the data volumes nowadays, content generally has to be selected in real time; not even the NSA can afford to store all the data on the Internet and the phone networks).

This fixed network is supplemented by tactical collection facilities as needed; Hagar describes, for example, the dispatch of Australian and New Zealand navy frigates to monitor domestic communications in Fiji during military coups in the 1980s. Koch and Sperber discuss U.S. and German installations in Germany in [725]; Fulghum describes airborne signals collection in [506]; satellites are also used to collect signals, and there are covert collection facilities too that are not known to the host country.

But despite all this huge capital investment, the most difficult and expensive part of the whole operation is traffic selection rather than collection [770]. Thus, contrary to one's initial 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. And if your cryptosecurity were perfect, you've just helped the enemy map your network, which means he can collect all the unencrypted traffic that you share with third parties.

Now 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.

19.3.2 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 State Department code book was stolen during World War 2 by the valet of the American ambassador to Rome, or errors in the manufacture and distribution of key material, as in the 'Venona' attacks on Soviet diplomatic traffic [676]. Even where attacks based on cryptanalysis have been possible, they have often been made much easier by operational errors, an example being the attacks on the German Enigma traffic during World War 2 [677]. The pattern continues to this day. The history of Soviet intelligence during the Cold War reveals that the USA's technological advantage 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 [77].

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 2, 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 [103]. 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 be simplified if the opponent uses cryptography — especially if they're competent and you can't read their encrypted traffic. This removes the ops/intel tension, and you switch to RDF or the destruction of protected links 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 useful 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. Cases where it is more effective than physical attack include satellite links, where the uplink can often 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 were anecdotes during the Bosnian war of Serbian information warfare cells attempting to DDoS NATO web sites.) This threat is still considered real enough that many Western countries have separate intranets for government and military use.

19.3.3 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 constant-rate pseudorandom bitstream on them at all times, regardless of whether there is any message traffic. But link layer encryption alone is not always enough, as enemy capture of a single node might put the whole network at risk.

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

- redundant 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;
- *low-probability-of-intercept* (LPI), *low-probability-of-position-fix* (LPPF) and anti-jam radio techniques.

The first two of these options are fairly straightforward to understand, and where they are 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).

A number of LPI/LPPF/antijam techniques 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 2, 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). I'll look at each of these three approaches in turn.

19.3.3.1 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. They 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 [763]. A frequency hopping radar was independently developed at about the same time by the Germans [1138].

Hoppers are resistant to jamming by an opponent who doesn't know the hop sequence. If the hopping is slow and a nearby opponent has capable equipment, then an option might be *follower jamming* — observing the signal and following it around the band, typically jamming each successive frequency with a single tone. However if the hopping is fast enough, or propagation delays are excessive, the opponent may have to jam much of the band, which requires much more power. 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 10MHz 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 or effectively follow the hop sequence, is *partial band jamming* — to jam enough of the band to introduce an unacceptable error rate in the signal.

Frequency hopping is used in some civilian applications, such as Bluetooth, where it gives a decent level of interference robustness at low cost. On the military side of things, although hoppers can give a large jamming margin, they give little protection against direction finding. A signal analysis receiver that sweeps across the frequency band of interest will usually intercept them (and depending on the relevant bandwidths, sweep rate and dwell time, it might intercept a hopping signal several times).

Since frequency hoppers are simple to implement and give a useful level of jam-resistance, they are often used in combat networks, such as man pack radios, with hop rates of 50–500 per second. To disrupt these 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. Hoppers are less 'LPI' than the techniques I'll describe next, as an opponent with a sweep receiver can detect the presence of a signal; and slow hoppers have some vulnerability to eavesdropping and direction finding, as an opponent with suitable wideband receiving equipment can often follow the signal.

19.3.3.2 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 (see Figures 19.1 and 19.2). This spreads the spectrum by increasing the bandwidth. The technique was first described by a Swiss engineer, Gustav Guanella, in a 1938 patent application [1138], and developed extensively in the USA 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 the opponent knows 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 tactic is to work in LPI mode until detected by the enemy (for example, when coming within radar range) and then boost transmitter power into antijam mode.

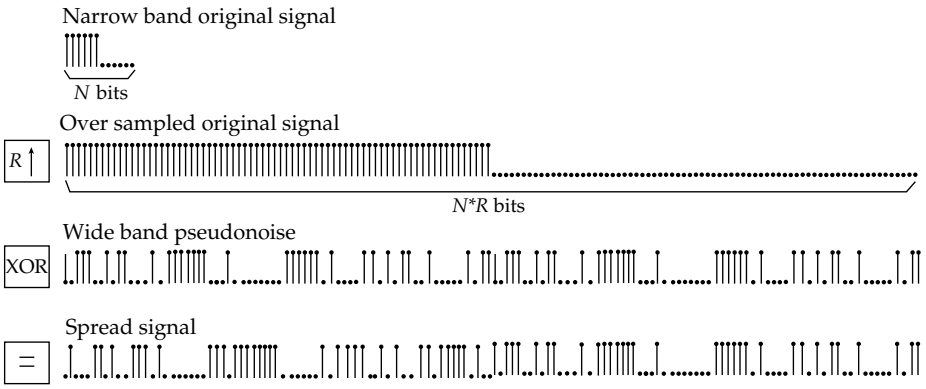

Figure 19.1: Spreading in DSSS (courtesy of Roche and Dugelay)

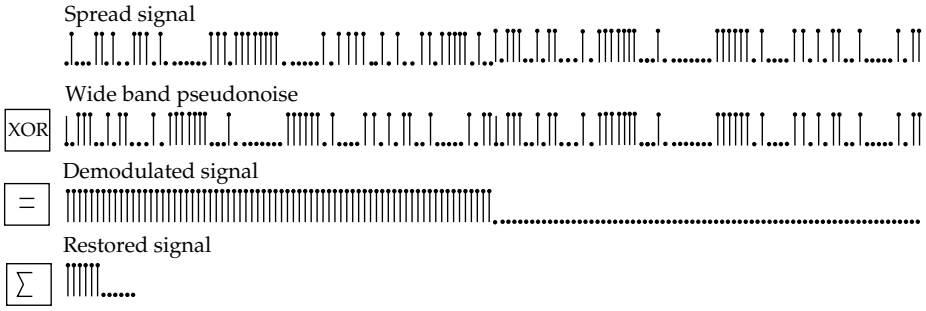

Figure 19.2: Unspreading in DSSS (courtesy of Roche and Dugelay)

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. Third-generation mobile phones in particular rely on CDMA for their performance.

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 [1026]; the engineering complexity is higher than with frequency hop for various reasons. For example, synchronization is particularly critical. One strategy is to have your users take turns at providing a reference signal. If your users have access to a reference time signal (such as GPS, or an atomic clock) you might rely on this; but 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 was reported in 2000 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 for 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 [1269]. Now GPS jammers are commodity items, and I'll discuss them in more detail below.

19.3.3.3 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*. They are usually not so jam-resistant (except insofar as the higher data rate spreads the spectrum) but can be even more difficult to detect than DSSS; 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. Really high-grade room bugs often use burst.

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 typically a third of a second and provides a temporary transmission path between a mother station and an area of maybe a hundred miles long and a few miles wide. The mother station transmits continuously; whenever one of the daughters is within such an area, it hears mother and starts to send packets of data at high speed, to which mother replies. With the low power levels used in covert operations one can achieve an average data rate of about 50 bps, with an average latency of about 5 minutes and a range of 500–1500 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 USAF in Alaska uses meteor scatter as backup communications for early warning radars. It's also used in civilian applications

such as monitoring rainfall in remote parts of the third world. 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 [1120].

19.3.3.4 Combining Covertness and Jam Resistance

There are some rather complex tradeoffs between different LPI, LPPF and jam resistance features, and other aspects of performance such as 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 follower. Some types of jamming translate between different modes: for example, an opponent with insufficient power to block a signal completely can do *partial time jamming* on DSSS by emitting pulses that cover a part of its utilized spectrum, and on frequency hop by *partial band jamming*.

There are also engineering tradeoffs. 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 [461].

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.

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

- The Jaguar tactical radio used by UK armed forces hops over one of nine 6.4 MHz bands, and also has an antenna with a steerable null which can be pointed at a jammer or at a hostile intercept station.
- Both DSSS and hopping are used with TDMA in *Joint Tactical Information Distribution System* (JTIDS) — a U.S. data link system used by AWACS to communicate with fighters [1121]. TDMA separates transmission from reception and lets users know when to expect their slot. It has a DSSS signal with 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 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 10MHz 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 is described in [530] 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. It was not in the end deployed.
- French tactical radios have remote controls. The soldier can use the handset a hundred yards from the radio. This means that attacks on the high-power emitter don't have to endanger the troops so much [348].

There are also some system level tricks, such as *interference cancellation* — here the idea is to communicate in a band which 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 [1074].

19.3.4 Interaction Between Civil and Military Uses

Civil and military uses of communications are increasingly intertwined. Operation Desert Storm (the First 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, and experts from various U.S. armed services claim that the effect of communications capability on the war was absolutely decisive [634]. It can be expected that both military and substate groups will attack civilian infrastructure to deny it to their opponents. Already, as I noted, satellite links are vulnerable to uplink jamming.

Another example of growing interdependency is given by the Global Positioning System, GPS. This started off 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 round 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 3 yards compared

with a claimed 8 yards for the standard military receiver [431]. Finally, in May 2000, President Clinton announced the end of selective availability. Various people have experimented with jamming GPS, which turns out to be not that difficult, and there has been some discussion of the systemic vulnerabilities that result from overreliance on it [490].

The U.S. government still reserves the right to switch off GPS, or to introduce errors into it, for example if terrorists were thought to be using it. But many diverse systems now depend on GPS, and many of them have motivated opponents; some countries are starting to use GPS to do road pricing, or to enforce parole terms on released prisoners via electronic ankle bracelets. As a result, GPS jammers appeared in car magazines in 2007 for $700; the price is bound to come down as truck drivers try to cheat road toll systems and car drivers try to beat pay-as-you-drive insurance schemes. Once their use becomes widespread, the consequences could be startling for other GPS users. Perhaps the solution lies in diversity: Russia has a separate navigation satellite system, and Europe's thinking of building one. Anyway, the security of navigation signals is starting to become a topic of research [751].

The civilian infrastructure also provides some defensive systems that government organizations (especially in the intelligence field) 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. The Tor network, pioneered by the U.S. Navy, does much the same for web pages, providing a low-latency way to browse the web via a network of proxies. I'll discuss this technology in more detail in section 23.4.2; the Navy makes it available to everyone on the Internet so as to generate lots of cover traffic to hide its own communications [1062]. Indeed, many future military applications are likely to use the Internet, and this will raise many interesting questions — ranging from the ethics of attacking the information infrastructure of hostile or neutral countries, to the details of how military traffic of various kinds can be hidden among civilian packets and bistreams.

There may indeed be some convergence. Although communications security on the net has until now been interpreted largely in terms of message confidentiality and authentication, the future may become much more like military communications in that jamming, service denial, anonymity, and deception will become increasingly important. I'll return to this theme later.

Next, 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 applies to both.)

19.4 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 1 (under the name of 'Asdic') [574]. Except in submarine warfare, the key sensor is radar. Although radar was invented in 1904 as a maritime anti-collision device, its serious development only occurred in the 1930s and it was used by all major participants in World War 2 [578, 670]. 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.

19.4.1 Types of Radar

A wide range of systems is in use, including search radars, fire-control radars, terrain-following radars, counter-bombardment 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 [1121].

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 which focuses on targets within a certain range of distances from the antenna; if the radar had to track all objects between (say) zero 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 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.

19.4.2 Jamming Techniques

Electronic attack techniques can be passive or active.

The earliest countermeasure to be widely used was *chaff* — thin strips of conducting foil that are cut to a half the wavelength of the target signal and then dispersed to provide a false return. Toward the end of World War 2, allied aircraft were dropping 2000 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; as the chaff is very light it comes to rest almost at once and can be distinguished fairly easily from moving targets.

Other decoy 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). These principles are quite general. Weapons that home in on their targets 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; as 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 that 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 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; as well as 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 non-coherent, in which case the jammer's 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 and 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, and 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 has to follow it. Such *follower jamming* can only make false targets that appear to be further away. So the counter-counter-countermeasure, or $(\text{counter})^3$-measure, is for the radar to have a *leading edge tracker*, which responds only to the first return pulse; and the $(\text{counter})^4$-measures can include jamming at

such a high power that the receiver's automatic gain control circuit is captured. An alternative is *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, so pilots could use this manoeuvre to break radar lock. And now of course, CPUs are powerful enough to manufacture realistic false returns.

19.4.3 Advanced Radars and Countermeasures

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

Pulse compression was first developed in Germany in World War 2, and 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 10–1000. 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 long before you detect him.

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 give 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 but 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 [807], and the UK 'Celldar' project aims to use the signals from mobile-phone masts for the same purpose [246]. The receivers, being passive, are hard to locate and attack; knocking out the system entails destroying major civilian infrastructure, which opponents will often prefer not to do for legal and propaganda reasons. Passive coherent location is effective against some kinds of stealth technology, particularly those that entail steering the aircraft so that it presents the nulls in its radar cross-section to visible emitters.

Attack and defence could become much more complex given the arrival of digital radio frequency memory and other software radio techniques. 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.

19.4.4 Other Sensors and Multisensor Issues

Much of what I've said about radar applies to sonar as well, and a fair amount to infrared. Passive decoys — flares — worked very well against early heat-seeking missiles which 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. They 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 which causes confusion. Some infrared defense systems are starting to employ lasers to disable the sensors of incoming weapons; and it's been admitted that a number of 'UFO' sightings were actually due to various kinds of jamming (both radar and infrared) [119].

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 I discussed in section 15.9, 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 then it will be easier for the enemy to jam you or sneak through.

System issues become more complex where the attacker himself is on a platform that's vulnerable to counter-attack, 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 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 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.

19.5 IFF Systems

Identify-Friend-or-Foe (IFF) systems are both critical and controversial, with a significant number of 'blue-on-blue' incidents in Iraq being due to equipment incompatibility between U.S. and allied forces. Incidents in which U.S. aircraft bombed British soldiers have contributed significantly to loss of UK public support for the war, especially after the authorities in both countries tried and failed to cover up such incidents out of a wish to both preserve technical security and also to minimise political embarrassment.

IFF goes back in its non-technical forms to antiquity; see for example the quote from Judges 12:5–6 at the head of Chapter 15 on identifying soldiers by whether they could pronounce 'Shibboleth'. World War 2 demonstrated the need for systems that could cope with radar; the Japanese aircraft heading toward Pearl Harbour were seen by a radar operator at Diamond Head but assumed to be an incoming flight of U.S. planes. Initial measures were procedural; returning bombers would be expected to arrive at particular times and cross the coast at particular places, while stragglers would announce their lack of hostile intent by some pre-arranged manoeuvre such as flying in an

equilateral triangle before crossing the coast. (German planes would roll over when the radio operator challenged them, so as to create a 'blip' in their radar cross-section.) There were also some early attempts at automation, with the 'Mark 1' system being mechanically tuned and not very usable. There were also early attempts at spoofing.

The Korean war saw the arrival on both sides of jet aircraft and missiles, which made it impractical to identify targets visually and imperative to have automatic IFF. Early systems simply used a vehicle serial number or 'code of the day', but this was wide open to spoofing, and the world's air forces started work on cryptographic authentication.

Since the 1960s, U.S. and other NATO aircraft have used the Mark XII system. This uses a crypto unit with a block cipher that is a DES precursor, and is available for export to non-NATO customers with alternative block ciphers. However, it isn't the cryptography that's the hard part, but rather the protocol problems discussed in Chapter 3. 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, then the radar's pulse repetition frequency (and thus it accuracy) would be degraded. So it's necessary to use short challenge-response pairs for radar security reasons, and many of them for cryptosecurity reasons. The Mark 12 sends 12–20 challenges in a series, and 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 focussed 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.)

This mechanism still doesn't completely stop 'ack wars' when two squadrons (or naval flotillas) meet each other. Meanwhile systems are becoming ever more complex. There's a program to create a NATO Mark XIIA that will be backwards-compatible with the existing Mark X/XII systems, and a U.S. Mark XV, both of which use spread-spectrum waveforms. The systems used in military aircraft also have compatibility modes with the civil systems used by aircraft to 'squawk' their ID to secondary surveillance radar. However, that's only for air-to-air IFF, and the real problems are now air-to-ground. NATO's IFF systems evolved for a Cold War scenario of thousands of tactical aircraft on each side of the Iron Curtain; how do they fare in a modern conflict like Iraq or Afghanistan?

Historically, about 10–15% of casualties were due to 'friendly fire' but in the First Gulf War this rose to 25%. Such casualties are more likely at the interfaces between air and land battle, and between sea and land,

because of the different services' way of doing things; joint operations are thus particularly risky. Coalition operations also increase the risk because of different national systems. Following this experience, several experimental systems were developed to 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 [1372]. An extension allows aircraft to broadcast targeting intentions on millimeter wave radio. The UK started developing a cheaper system in which friendly vehicles carry an LPI millimeter-wave transmitter, and shooters carry a directional receiver [599]. (Dismounted British foot soldiers, unlike their American counterparts, were not deemed worthy of protection.) A prototype system was ready in 2001 but not put into production. Other countries started developing yet other systems.

But when Gulf War 2 came along, nothing decent had been deployed. A report from Britain's National Audit Office from 2002 describes what went wrong [930]. In a world where defence is purchased not just by nation states, and not just by services, but by factions within these services, and where legislators try to signal their 'patriotism' to less-educated voters by blocking technical collaboration with allies ('to stop them stealing our jobs and our secrets'), it's hard. The institutional and political structures just aren't conducive to providing defense 'public goods' such as a decent IFF system that would work across NATO. And NATO is a broad alliance; as one insider told me, ''Trying to evolve a solution that met the aspirations of both the U.S. at one extreme and Greece (for example) at the other was a near hopeless task.''

Project complexity is one issue: it's not too hard to stop your air force planes shooting each other, it's a lot more complex to stop them shooting at your ships or tanks, and it's much harder still when a dozen nations are involved. Technical fixes are still being sought; for example, the latest U.S. software radio project, the Joint Tactial Radio System (JTRS, or 'jitters'), may eventually equip all services with radio that interoperate and do at least two IFF modes. However, it's late, over budget, and fragmented into subprojects managed by the different services. There are also some sexy systems used by a small number of units in Iraq that let all soldiers see each others' positions superimposed in real time on a map display on a helmet-mounted monocle. They greatly increase force capability in mobile warfare, allowing units to execute perilous manoevres like driving through each others' kill zones, but are not a panacea in complex warfare such as Iraq in 2007: there, the key networks are social, not electronic, and it's hard to automate networks with nodes of unknown trustworthiness [1116].

In any case, experience so far has taught us that even with 'hard-core' IFF, such as where ships and planes identify each other, the hardest issues weren't technical but to do with economics, politics and doctrine. Over more than a

decade of wrangling within NATO, America wanted an expensive high-tech system, for which its defense industry was lobbying hard, while European countries wanted something simpler and cheaper that they could also build themselves, for example by tracking units through the normal command-and-control system and having decent interfaces between nations. But the USA refused to release the location of its units to anyone else for 'security' reasons. America spends more on defense than its allies combined and believed it should lead; the allies didn't want their own capability further marginalised by yet more dependence on U.S. suppliers.

Underlying doctrinal tensions added to this. U.S. doctrine, the so-called 'Revolution in Military Affairs' (RMA) promoted by Donald Rumsfeld and based on an electronic system-of-systems, was not only beyond the allies' budget but was distrusted, based as it is on minimising one's own casualties through vast material and technological supremacy. The Europeans argued that one shouldn't automatically react to sniper fire from a village by bombing the village; as well as killing ten insurgents, you kill a hundred civilians and recruit several hundred of their relatives to the other side. The American retort to this was that Europe was too weak and divided to even deal with genocide in Bosnia. The result was deadlock; countries decided to pursue national solutions, and no real progress has been made on interoperability in twenty years. Allied forces in Iraq and Afghanistan were reduced to painting large color patches on the roofs of their vehicles and hoping the air strikes would pass them by. U.S. aircraft duly bombed and killed a number of allied servicemen, which weakened the alliance. Perhaps we'll have convergence in the long run, as European countries try to catch up with U.S. military systems, and U.S. troops revert to a more traditional combat mode as they discover the virtues of winning local tribal allies in the fight against Al-Qaida in Iraq. However, for a converged solution to be stable, we may well need some institutional redesign.

19.6 Improvised Explosive Devices

A significant effort has been invested in 2004–7 in electronic-warfare measures to counter the improvised explosive devices (IEDs) that are the weapon of choice of insurgents in Iraq and, increasingly, Afghanistan. Since the first IED attack on U.S. forces in March 2003, there have been 81,000 attacks, with 25,000 in 2007 alone. These bombs have become the 'signature weapon' of the Iraq war, as the machine-gun was of World War 1 and the laser-guided bomb of Gulf War I. (And now that unmanned aerial vehicles are built by hobbyists for about $1000, using model-aircraft parts, a GPS receiver and a Lego Mindstorms robotics kit, we might even see improvised cruise missiles.)

Anyway, over 33,000 jammers have been made and shipped to coalition forces. The Department of Defense spent over $1bn on them in 2006, in an operation that, according to insiders, 'proved the largest technological challenge for DOD in the war, on a scale last experienced in World War 2' [94]. The overall budget for the Pentagon's Joint IED Defeat Organization was claimed to almost $4bn by the end of 2006. Between early 2006 and late 2007, the proportion of radio-controlled IEDs dropped from as much as 70% to 10%; the proportion triggered by command wires increased to 40%.

Rebels have been building bombs since at least Guy Fawkes, who tried to blow up Britain's Houses of Parliament in 1605. Many other nationalist and insurgent groups have used IEDs, from anarchists through the Russian resistance in World War 2, the Irgun, ETA and the Viet Cong to Irish nationalists. The IRA got so expert at hiding IEDs in drains and culverts that the British Army had to use helicopters instead of road vehicles in the 'bandit country' near the Irish border. They also ran bombing campaigns against the UK on a number of occasions in the twentieth century. In the last of these, from 1970–94, they blew up the Grand Hotel in Brighton when Margaret Thatcher was staying there for a party conference, killing several of her colleagues; later, London suffered two incidents in which the IRA set off truckloads of home-made explosive causing widespread devastation. The fight against the IRA involved 7,000 IEDs, and gave UK defense scientists much experience in jamming: barrage jammers were fitted in VIP cars that would cause IEDs to go off either too early or too late. These were made available to allies; such a jammer saved the life of President Musharraf of Pakistan when Al-Qaida tried to blow up his convoy in 2005.

The electronic environment in Iraq turned out to be much more difficult than either Belfast or the North-West Frontier. Bombers can use any device that will flip a switch at a distance, and employed everything from key fobs to cellphones. Meanwhile the RF environment in Iraq had become complex and chaotic. Millions of Iraqis used unregulated cellphones, walkie-talkies and satellite phones, as most of the optical-fibre and copper infrastructure had been destroyed in the 2003 war or looted afterwards. 150,000 coalition troops also sent out a huge variety of radio emissions, which changed all the time as units rotated. Over 80,000 radio frequencies were in use, and monitored using 300 databases — many of them not interoperable. Allied forces only started to get on top of the problem when hundreds of Navy electronic warfare specialists were deployed in Baghdad; after that, coalition jamming efforts were better coordinated and started to cut the proportion of IEDs detonated by radio.

But the 'success' in electronic warfare hasn't translated into a reduction in allied casualties. The IED makers have simply switched from radio-controlled bombs to devices detonated by pressure plates, command wires, passive infrared or volunteers. The focus is now shifting to a mix of tactics: 'right of boom' measures such as better vehicle armor, and 'left of boom' measures

such as disrupting the bomb-making networks (Britain and Israel had for years targeted bombmakers in Ireland and Lebanon respectively). Better armor at least is having some effect: while in 2003 almost every IED caused a coalition casualty, now it takes four devices on average [94]. Armored vehicles were also a key tactic in other insurgencies. Network disruption, though, is a longer-term play as it depends largely on building up good sources of human intelligence.

19.7 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 [670]. 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 2, the invention of the cavity magnetron had made it possible to build radars powerful enough to damage unprotected

electronic circuitry at 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. In fact, the banks' underground server farms would likely be unaffected; the real damage would be to everyday electronic devices. For example, some electronic car keys are so susceptible to RF that they can be destroyed if left next to a cell phone [1073]. Replacing the millions of gadgets on which a city's life depends would be extremely tiresome.

For battlefield use, it's useful if the weapon can be built into a standard bomb or shell casing rather than having to be truck-mounted. The Soviets are said to have built high-energy RF (HERF) devices, and the U.S. responded with its own arsenal: a device called Blow Torch was tried in Iraq as a means of frying the electronics in IEDs, but it didn't work well [94]. There's a survey of usable technologies at [737] that describes how power pulses in the Terawatt range can be generated using explosively-pumped flux compression generators and magnetohydrodynamic devices, as well as by more conventional high-power microwave devices.

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. 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, the antenna will usually just be a few meters. According to the cited paper, EMP bombs need to be dropped from aircraft and deploy antennas before detonation in order to get decent coupling, and even so are lethal to ordinary electronic equipment for a radius of only a few hundred meters. NATO planners concluded that military command and control systems that were already hardened for nuclear EMP should be unaffected.

And as far as terrorists are concerned, I wrote here in the first edition of this book: '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!' That was published a few months before 9/11. Of course, a Boeing 767 will do more damage than a truck bomb, but a truck bomb still does plenty, as we see regularly in Iraq, and even small IEDs of the kind used by Al-Qaida in London in 2005 can kill enough people to have a serious political effect. In addition, studies of the psychology of terror support the view that lethal attacks are much more terrifying than nonlethal ones almost regardless of the economic

damage they do (I'll come back to this in Part III). So I expect that terrorists will continue to prefer a truckload of fertiliser to a truckload of magnetrons.

There remains one serious concern: that the EMP from a single nuclear explosion at an altitude of 250 miles would do colossal economic damage, while killing few people directly [80]. This gives a blackmail weapon to countries such as Iran and North Korea with nuclear ambitions but primitive technology otherwise. North Korea recently fired a missile into the sea near Japan, which together with their nuclear test sent a clear signal: 'We can switch off your economy any time we like, and without directly killing a single Japanese civilian either'. And how would Japan respond? (They're hurriedly testing anti-missile defences.) What, for that matter, would the USA do if Kim Jong-Il mounted a missile on a ship, sailed it towards the Panama Canal, and fired a nuke 250 miles above the central United States? That could knock out computers and communications from coast to coast. A massive attack on electronic communications is more of a threat to countries such as the USA and Japan that depend on them, than on countries such as North Korea (or Iran) that don't.

This observation goes across to attacks on the Internet as well, so let's now turn to 'Information Warfare'.

19.8 Information Warfare

From about 1995, the phrase *Information warfare* came into wide use. Its popularity was boosted 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 [825].) 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 built on.

After 9/11, information warfare was somewhat eclipsed as the security-industrial complex focussed on topics from airport screening to the detection of improvised explosive devices. But in April 2007, it was thrust back on the agenda by events in Estonia. There, the government had angered Russia by moving an old Soviet war memorial, and shortly afterwards the country was subjected to a number of distributed denial-of-service attacks that appeared

to originate from Russia [359]. Estonia's computer emergency response team tackled the problem with cool professionalism, but their national leadership didn't. Their panicky reaction got world headlines [413]; they even thought of invoking the NATO treaty and calling for U.S. military help against Russia.

Fortunately common sense prevailed. It seems that the packet storms were simply launched by Russian botnet herders, reacting to the news from Estonia and egging each other on via chat rooms, rather than being an act of state aggression; the one man convicted of the attacks was an ethnic Russian teenager in Estonia itself. There have been similar tussles between Israeli and Palestinian hackers, and between Indians and Pakistanis. Estonia also had some minor street disturbances caused by rowdy ethnic Russians objecting to the statue's removal; 'Web War 1' seems to have been the digital equivalent. Since then, however, there have been press reports alleging Chinese attacks on government systems in both the USA and the UK, including service-denial attacks and attempted intrusions, causing 'minor administrative disruptions' [973]. Defense insiders leak reports saying that China has a massive capability to attack the West [1063]. Is this serious, or is it just the agencies shaking the tin for more money?

But what's information warfare anyway? There is little agreement on definitions. The conventional view, arising out of Desert Storm, was expressed by Whitehead [1314]:

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

Meanwhile, 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.

19.8.1 Definitions

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

- that 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;
- that 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 is observed, for example, that the Internet was designed to withstand thermonuclear bombardment, but was knocked out by the Morris worm;

- that it extends the electronic warfare doctrine of controlling the electromagnetic spectrum to control 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. 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 by Dorothy Denning [370] 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), but propaganda too. In a later article she discussed the role of the net in the propaganda and activism surrounding the Kosovo war [371]. 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 given by Edward Waltz [1314]. 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 but set forth a first attempt to formulate a military doctrine of information operations.

19.8.2 Doctrine

When writers such as Denning and Waltz include propaganda operations in information warfare, the cynical defense insider will 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 2 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 [320] — 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 a 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 comes 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 bomber aircraft get through unscathed, but is 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, more developed countries are more exposed. The power grid in the USA or the UK is likely to be much more computerized than that in a developing country.
- Finally, if such an attack causes the deaths of several dozen people in hospitals, the Iranians aren't likely to see the matter as being much different from a conventional military attack that killed the same number of people. Indeed, if information war targets civilians to an even 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.

19.8.3 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 [761].) Things are even worse when intelligence services are involved, as they don't train with warfighters in peacetime and thus 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 [103]. 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 [1115].

At the technical level, there are many concepts which 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). The use of 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, in order to make life harder for the virus scanner vendors; similarly, radar designers use very diverse waveforms in order 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, 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 with 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 boosting power; similarly, when a non-existent 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 want a different line (or the attacker will keep on trying). Something like 'Sorry, the items you have requested are temporarily out of stock and should be dispatched 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 to defend against an incoming cruise missile knocks out the anti-aircraft gun. The side-effects of defenses can also be exploited. The most common case on the net is the mail bomb in

which an attacker forges offensive newsgroup messages that 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 are cheaper, can be used against multiple threats, and have reduced political consequences. But damage assessment is hard, and you may just divert the weapon to another target. As most information war is soft-kill, these comments can be expected to go across too.

19.8.4 Differences Between E-war and I-war

As well as similarities, there are differences 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 first of these: in air combat, most naval engagements, and the desert. In forests, mountains and cities, the man with the AK47 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, mountains and cities' are the large numbers of insecure hosts belonging to friendly or neutral civilians and organizations. The distributed denial of service attack, in which millions of innocent machines are subverted and used to bombard a target website with traffic, has no real analogue in the world of electronic warfare: yet 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, which makes little difference when fighting another large country with similarly incompatible systems, but can leave them at a disadvantage to a small group with simple coherent systems.
- Anyone trying to attack the USA in future is unlikely to repeat Saddam Hussein's mistake of taking on the West in a tank battle. Asymmetric conflict is now the norm, and although cyberspace has some potential here, physical attacks have so far got much more traction — whether at the Al-Qaida level of murderous attacks, or at the lower level of (say) animal rights activists, who set out to harass people rather than murder them and thus stay just below the threshold at which a drastic state

response would be invoked. A group that wants to stay at this level — so that its operatives risk short prison sentences rather than execution — can have more impact if it uses physical as well as electronic harassment.

As a member of Cambridge University's governing body, the Council, I was subjected for some months to this kind of hassle, as animal rights fanatics protested at our psychology department's plans to construct a new building to house its monkeys. I also watched the harassment's effects on colleagues. Spam floods were easily enough dealt with; people got much more upset when protesters woke them and their families in the small hours, by throwing rocks on their house roofs and screaming abuse. I'll discuss this later in Part III.

- 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 tools are available universally, and for free, has few analogues in meatspace. You might draw a comparison with the lawless areas of countries such as Afghanistan where all men go about armed. But the damage done by Russian script kiddies to Estonia was nothing like the damage done to allied troops by Afghan tribesmen — whether in the present Afghan war or in its nineteenth century predecessors.

19.9 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 if information warfare takes off, and turns from a fashionable concept into established doctrine and practice, these lessons will become important for engineers.

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 non-technical) introduction to radar is by P. S. Hall [578]. The best all-round reference for the technical aspects of electronic warfare, from radar through stealth to EMP weapons, is by Curtis Schleher [1121]; a good summary was written by Doug Richardson [1074]. The classic introduction to the anti-jam properties of spread spectrum sequences is by Andrew Viterbi [1301]; the history of spread spectrum is ably told by Robert Scholtz [1138]; the classic introduction to the mathematics of spread spectrum is by Raymond Pickholtz, Donald Schilling and Lawrence Milstein [1026]; while the standard textbook is by Robert Dixon [393]. The most thorough reference on communications jamming is by Richard Poisel [1029]. An overall history of British electronic warfare and scientific intelligence, which was written by a true insider and gives a lot of insight not just into how the technology developed but also into strategic and tactical deception, is by R. V. Jones [670, 671].