**Chapter 23**

**Electronic and Information**  
 **Warfare**

**All warfare is based on deception ... hold out baits to entice**

**the enemy. Feign disorder, and crush him.**

– Sun Tzu

**Force, and Fraud, are in warre the two Cardinal Virtues.**

– Thomas Hobbes

**23.1** **Introduction**

For decades, electronic warfare was a separate subject from computer security,  
 even though they use some common technologies. This started to change in  
 the last years of the twentieth century as the Pentagon started to fuse elements  
 of the two disciplines into the new subject of *information warfare*, followed by  
 Russia and China. The Russian denial-of-service attacks on Estonia in 2007  
 put it ﬁrmly on many policy agendas; Stuxnet moved it into prime time; and  
 the Russian interference in two big political events of 2016, the UK Brexit  
 referendum and the US election, taught legislators that it could cost them their  
 jobs.

There are other reasons why some knowledge of electronic warfare is im-

portant 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 was the ﬁrst area of  
 electronic security to have experienced a lengthy period of coevolution of attack  
 and defense involving capable motivated opponents, giving rise to deception  
 strategies and tactics of a unique depth and subtlety. Although the subject lan-  
 guished after the end of the Cold War in 1989, it has revived recently as China  
 works to become a peer competitor to the USA, as Russia modernises its armed  
 forces, and as AI ﬁnds its way into radar, sonar and related systems. Warfare  
 is about to get hi-tech again, unlike in 2000-2020 with its emphasis on spooks  
 hacking people’s phones and special forces then kicking down their doors.

704

*23.2. BASICS*

Electronic warfare was also our ﬁrst teacher about service-denial attacks, a

topic that computer security people ignored for years, and about hybrid attacks  
 that involve both direct and psychological factors. Finally, many of the tech-  
 niques evolved to defeat enemy radars, including various kinds of decoys and  
 jamming, have interesting parallels in the new ‘information warfare’ world of  
 fake news, troll farms and postmodern propaganda.

**23.2** **Basics**

While old-fashioned computer security was about conﬁdentiality, integrity and  
 availability, electronic warfare has this the other way round. 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 op-

erationally valuable information from the enemy’s use of his electronic  
 systems.

At the level of doctrine, electromagnetic warfare is generally considered to

consist of

*• electronic attack*, such as jamming enemy communications or radar, and

*• electronic protection*, which is about retaining some radar and communica-  
 sistant to jamming, through hardening equipment to resist high-power mi-  
 crowave attack, to the destruction of enemy jammers using anti-radiation  
 missiles; and

*• electronic support*, which supplies the necessary intelligence and threat  
 to search for, identify and locate sources of intentional and unintentional  
 electromagnetic energy.

These deﬁnitions are taken from Schleher [1662]. The traditional topic of

cryptography, namely *communications security* (Comsec), is only a small part  
 of electronic protection, just as it is only a small part of information protec-  
 tion in modern civilian systems. Electronic support includes *signals intelli-*

*gence*, or Sigint, which consists of *communications intelligence* (Comint) and  
 *electronic intelligence* (Elint). The former collects enemy communications, in-  
 cluding both message content and traffic data about which units are communi-  
 cating, 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 their perceptions in order to degrade the accuracy of their  
 intelligence and target acquisition. Its effective use depends on clarity about who

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 705 | Ross Anderson |

*23.3. COMMUNICATIONS SYSTEMS*

(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 be destroyed (*hard kill*). Successful electronic warfare depends  
 on using the available tools in a coordinated way.

Electronic weapon systems are like other weapons in that there are *sensors*,

such as radar, infrared and sonar; *communications* links which take sensor data  
 to the command and control center; and output devices such as jammers, lasers,  
 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 electronic warfare, we’ll look at the lessons we might take over to  
 information warfare.

**23.3** **Communications Systems**

Military communications were dominated by physical dispatch until about 1860,  
 then by the telegraph until 1915, and then by the telephone and radio until after  
 the end of the Cold War [1380]. 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. There  
 are also ﬁxed links including the Internet and classiﬁed IP networks. Without  
 situational awareness and the means to direct forces, the commander is likely  
 to be ineffective. But the need to secure communications is pervasive, and the  
 threats are very diverse.

*•* One obvious type of traffic is the communications between ﬁxed sites such  
 ical threat here was that the cipher security might be penetrated and  
 the orders, situation reports and so on compromised, whether as a re-  
 sult 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. Cipher security may include  
 protection against traffic analysis (such as by constant bitrate encryption  
 of some links) as well as of the transmitted message conﬁdentiality and  
 authenticity. The secondary threat is that the link might be disrupted,  
 whether by destruction of cables or relay stations, or by traffic ﬂooding  
 where resources are shared.

*•* There are more stringent requirements for communications with covert  
 location security is important. Agents have to take steps to minimize the  
 risk of being caught as a result of communications monitoring. If they send  
 messages using a medium the enemy can monitor, such as the Internet or

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 706 | Ross Anderson |

*23.3. COMMUNICATIONS SYSTEMS*

radio, then some effort may go into frustrating traffic analysis and radio  
 direction ﬁnding.

*•* Tactical communications, such as between HQ and a platoon in the ﬁeld,  
 ﬁnding is still an issue, but jamming may be at least as important, and de-  
 liberately deceptive messages may also be a problem. By the 1980s, there  
 was equipment that enabled 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 [730]. As  
 voice morphing techniques are developed using deepfake techniques from  
 machine learning, the risk of spooﬁng attacks on communications will in-  
 crease. So cipher security may increasingly include authenticity as well as  
 conﬁdentiality and covertness.

*•* Control and telemetry communications, such as signals sent from an air-  
 and modiﬁcation. It would also be nice 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. A common solution is  
 to make the communications adaptive – to start off in a low-probability-of-  
 intercept mode, but ramp up the power as 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 subtle ways. For example, one radio designed for use by dissi-  
 dent 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 to work  
 harder at 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.  
 According to Soviet doctrine, a comprehensive and successful attack on a mil-  
 itary 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 their traffic over a third of their in-  
 stalled capacity [1156]. 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 [1380].

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 Gulf War 1. Of course, attacking an army’s  
 command structures is much older; it’s basic common sense to shoot at an  
 officer before shooting at his men.

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 707 | Ross Anderson |

*23.3. COMMUNICATIONS SYSTEMS*

**23.3.1** **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 phone networks and the Internet.

In the case of radio signals, communications intelligence agencies collect a

huge variety of signal types and build extensive databases of which stations or  
 services use which frequencies and how. It is often possible to identify individual  
 equipment by signal analysis. The giveaways 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*  
 (RFID) technology was declassiﬁed in the mid-1990s for use in identifying cloned  
 cellphones [776, 1662]. 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 [1224].

*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 be-

fore having to move. Modern monitoring stations use *time difference of arrival*  
 (TDOA) to locate a suspect signal accurately and automatically by comparing  
 the phase of the signals received at two sites; nowadays, anything more than a  
 second or so of transmission can be a giveaway.

*Traffic analysis* – looking at the number of messages by source and destina-

tion – can also give very valuable information. Imminent attacks were signalled  
 in World War 1 by a greatly increased volume of radio messages, and more re-  
 cently by increased pizza deliveries to the Pentagon. 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 the late 1990s, traffic analysis was the domain of intelligence  
 agencies – when NSA ops people referred to themselves as ‘hunter-gatherers’,  
 traffic analysis was much of the ‘hunting’. In this century, however, traffic

analysis has come out of the shadows and become a major subject of study; I  
 discuss this in the context of law-enforcement and intelligence surveillance in  
 section 26.2.2.

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 ev-  
 eryone 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 an-  
 alyze, and repeat the procedure on each remaining number. Having done this  
 procedure recursively two or three times, you amass 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 approx-  
 imation to Alice’s network, and reﬁne it by collating it with other intelligence  
 sources. *Covert community detection* became a very hot topic after 9/11, and

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 708 | Ross Anderson |

*23.3. COMMUNICATIONS SYSTEMS*

researchers have tried all sorts of hierarchical clustering and graph partitioning  
 methods to the problem. One leading algorithm is by Mark Newman [1434]; it  
 uses spectral methods to partition a network into its natural communities so as  
 to maximise modularity. The standard reference on such techniques is Easley  
 and Kleinberg [599].

But even given good mathematical tools for analysing abstract networks,

reality is messier. People can have several numbers, and they also 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 has too many active contacts to analyse  
 effectively). Also, you’ll 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 hacked PBXs  
 and encrypted messaging services such as Signal. Tying IP addresses to people  
 is even harder; ISPs don’t always keep the Radius logs for long. I discuss all  
 these issues in more detail elsewhere, including Ed Snowden’s revelations about  
 what the NSA did in section 2.2.1 and the history of the Five Eyes intelligence  
 sharing agreement in section 26.2.6. 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’re not a universal answer for the crook as

the discipline needed to use anonymous communications properly is beyond  
 most criminals. It was reported, for example, that one of the alleged 9/11

masterminds 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, as revealed by Ed Snowden in 2013 and  
 described in section 2.2.1. Even before then, we knew the broad picture, thanks  
 to a long series of leaks and work by investigative journalists. A 1996 book by  
 Nicky Hager [849] described a Five Eyes collection network. Known as *Echelon*,  
 this consisted of a number of ﬁxed collection stations that monitored phone, fax  
 and data traffic with computers called *dictionaries* that searched passing traffic  
 for interesting phone numbers, network addresses and machine-readable content;  
 this traffic selection was driven by search strings entered by intelligence analysts.  
 Two years before Google was founded, Echelon was already a kind of Google for  
 the world’s phone system; the 2013 system described by Snowden extends this to  
 IP networks and to the greater traffic volumes of today. It has become a massive  
 distributed search engine with over a hundred nodes worldwide. Ingested traffic  
 is ﬁrst subject to massive data reduction – the video and the broadcast stuff  
 gets thrown away – and then content is kept for a period of a few days in case  
 anyone wants it. Traffic data is also kept, but for longer.

This ﬁxed network is supplemented by tactical collection facilities as needed.

Hager described, 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 US and German installations in Germany  
 in the 1990s in [1062]; Fulghum describes airborne signals collection in [730];

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 709 | Ross Anderson |

*23.3. COMMUNICATIONS SYSTEMS*

satellites are also used to collect signals, and there are covert collection facilities  
 too that are not known to the host country. For example, in section 2.2.1.9 I  
 describe Operation Socialist, where GCHQ hacked the Belgian phone company  
 to get access to third-party mobile-phone traffic routed through Belgium and  
 also to the communications of EU institutions in Brussels.

Since the Snowden revelations, over half of IP traffic has been encrypted,

which has shifted the focus of intelligence and law enforcement somewhat to  
 collection from endpoints. This brings us to the topic of attacks.

**23.3.2** **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 been on the supply or custody of  
 equipment or key material. Examples include the theft of the State Department  
 code book during World War 2 by the valet of the American ambassador to  
 Rome [1001]; errors in the manufacture and distribution of one-time pads lead-  
 ing to the ‘Venona’ attacks on Soviet diplomatic traffic [1001]; and the covert  
 ownership of the Swiss company Crypto AG by the CIA and Germany’s Bun-  
 desnachrichtendienst, which I discuss in section 26.2.7.1. Ed Snowden disclosed  
 the theft by GCHQ of the card personalisation ﬁles from Gemplus, which com-  
 promised the keys in millions of SIM cards, giving the intelligence community  
 access to the traffic of millions of mobile phones. Even where attacks based  
 on cryptanalysis have happened, they have often been made much easier by  
 operational errors, as with the attacks on the German Enigma traffic during  
 World War 2 [1002], or by political interference with cryptography. This can  
 be overt, as with export controls (see sections 4.3.1 and 26.2.9), or subtle, as  
 with standards for random number generators (see section 2.2.1.5) and VPNs  
 (section 2.2.1.7). Such activities are known by the agencies as ‘crypto enabling’  
 and their budgets are in nine ﬁgures. Other states play similar games: the

history of Soviet intelligence during the Cold War reveals that the USA’s tech-  
 nological advantage was largely nulliﬁed by Soviet skills in ‘using Humint in  
 Sigint support’ – recruiting traitors who sold key material, such as the Walker  
 family [118]. More recently, Chinese attacks on cloud service providers and on  
 key assets such as the Office of Personnel Management – which got them the  
 clearance data ﬁles on essentially all US government employees – were described  
 in section 2.2.2.

Second, access to content is often not the desired result. In tactical sit-

uations, 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 authenti-  
 cation techniques were invented and defeated. 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 [150]. Compro-  
 mises 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!

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 710 | Ross Anderson |

*23.3. COMMUNICATIONS SYSTEMS*

Matters can be simpliﬁed if the opponent uses cryptography – especially if

they’re competent and you can’t read their traffic. This removes the ops/intel  
 tension, so you switch to RDF or the destruction of protected links as appro-  
 priate. This can involve the hard-kill approach of digging up cables or bombing  
 telephone exchanges (both of which the Allies did during Gulf War 1), the soft-  
 kill approach of jamming, or whatever combination is effective. 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 infor-  
 mation 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.

**23.3.3** **Protection techniques**

So communications security techniques involve not just protecting authenticity  
 and conﬁdentiality, but also preventing traffic analysis, direction ﬁnding, jam-  
 ming and physical destruction. Encryption can stretch to the ﬁrst of these if  
 applied at the link layer, so that all links have a constant-rate pseudorandom  
 bitstream on them at all times. But link-layer encryption is tricky over radio,  
 because of the trade-off between synchronisation and jamming; and on its own  
 it 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  
 high frequencies;

*• low-probability-of-intercept* (LPI), *low-probability-of-position-ﬁx* (LPPF) and

The ﬁrst two of these options are fairly straightforward, and where they’re

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

(brieﬂy).

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 711 | Ross Anderson |

*23.3. COMMUNICATIONS SYSTEMS*

A number of LPI/LPPF/antijam techniques go under the generic name of

*spread spectrum* communications. They include *frequency hoppers*, *direct se-*

*quence spread spectrum* (DSSS) and *burst transmission*. From beginnings around  
 World War 2, spread spectrum has spawned a substantial industry and the tech-  
 nology (especially DSSS) has been applied to numerous other problems, ranging  
 from high resolution ranging (in the GPS system) through radio protocols such  
 as Bluetooth. I’ll look at each of these three approaches in turn.

**23.3.3.1** **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 [1702]. A  
 frequency-hopping radar was independently developed at about the same time  
 by the Germans [1682].

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 107*/*102 = 105 = 50dB. 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 e↵ectively 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

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 712 | Ross Anderson |

*23.3. COMMUNICATIONS SYSTEMS*

Narrow band original signal

*N* bits

Over sampled original signal

|  |
| --- |
| *R* |

*N\*R*bits

Wide band pseudonoise

|  |
| --- |
| XOR |

Spread signal

|  |
| --- |
|  |

Figure 23.1: – spreading in DSSS (courtesy of Roche and Dugelay)

Spread signal

Wide band pseudonoise

|  |
| --- |
| XOR |

Demodulated signal

|  |
| --- |
|  |

Restored signal

Figure 23.2: – unspreading in DSSS (courtesy of Roche and Dugelay)

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.

**23.3.3.2** **DSSS**

In direct-sequence spread spectrum, we multiply the information-bearing se-  
 quence by a much higher rate pseudorandom sequence, usually generated by  
 some kind of stream cipher (see Figures 23.1 and 23.2). This spreads the spec-  
 trum by increasing the bandwidth. The technique was ﬁrst described by a Swiss  
 engineer, Gustav Guanella, in a 1938 patent application [1682], 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 sig-  
 niﬁcantly 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.

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 713 | Ross Anderson |

*23.3. COMMUNICATIONS SYSTEMS*

There is a large literature on DSSS, and the techniques have now been taken

up by the commercial world as *code division multiple access* (CDMA) in various  
 mobile radio and phone systems.

DSSS is sometimes referred to as “encrypting the RF” and it comes in a

number of variants. For example, when the underlying modulation scheme is  
 FM rather than AM it’s called *chirp*. The classic introduction to the underly-  
 ing mathematics and technology is [1525]; 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 [1918]. Now GPS jammers are commodity items and I’ll  
 discuss them in more detail a little later in this chapter.

**23.3.3.3** **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 typi-  
 cally 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 daugh-  
 ters 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 av-  
 erage latency of about 5 minutes and a range of 500–1500 miles. Meteor burst  
 communications are used by special forces, and in civilian applications such as  
 monitoring rainfall in remote parts of the third world. With higher power levels,  
 and in higher latitudes, average data rates can rise into the tens of kilobits per  
 second, and the USAF in Alaska uses such systems as backup communications  
 for early warning radars. 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 [1661].

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 714 | Ross Anderson |

*23.3. COMMUNICATIONS SYSTEMS*

**23.3.3.4** **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 simultane-  
 ously. 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 be-  
 tween 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 the spectrum it uses, just like partial band jamming  
 of frequency hop.

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 [673].

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

*•* Both DSSS and hopping are used with TDMA in *Link 16*, as it’s known  
 *Link* (TADIL), and was previously known as the *Joint Tactical Informa-*  
 *tion Distribution System* (JTIDS) [1662]. TDMA separates transmission  
 from reception and lets users know when to expect their slot. It has a  
 DSSS signal with a 57.6KHz data rate and a 10MHz chip rate (and so a  
 jamming margin of 36.5dB), which hops around in a 255MHz 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 255MHz. Development started in 1967 with Gordon Welchman, who  
 also broke German ciphers at Bletchley during World War 2; after pilot  
 projects in the 1970s, serious development started in the 1980s and the  
 system was fully deployed from about 2000, seeing use in Afghanistan and  
 Iraq [1956].

*•* The US armed forces have been supported by a series of satellite com-  
 a geostationary orbit. The effect of the narrow beam is that users can  
 operate within three miles of the enemy without being detected. Jam pro-  
 tection is from hopping: its channels hop several thousand times a second  
 in bands of 2GHz.

*•* French tactical radios have remote controls. The soldier can use the hand-

high-power emitter don’t have to endanger the troops so much [514].

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 715 | Ross Anderson |

*23.3. COMMUNICATIONS SYSTEMS*

There are also some system-level tricks, such as *interference cancellation* –

where you communicate in a band which you’re jamming with a waveform 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 them to spread their available power  
 over a larger bandwidth, and can make signals intelligence harder too [1601].

**23.3.4** **Interaction between civil and military uses**

Civil and military communications are increasingly intertwined. Operation

Desert Storm (Gulf War 1 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 US armed services claim that the effect of communications capability  
 on the war was decisive [942].

Another example of growing interdependency is the Global Positioning Sys-

tem, GPS. This started off as a US 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  
 Gulf War 1 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 in civil aviation that the FAA helped ﬁnd ways to defeat selective avail-  
 ability and give an accuracy of about 3 yards compared with a claimed 8 yards  
 for the standard military receiver [630]. Finally, in May 2000, President Clinton  
 announced the end of selective availability.

The US government still reserves the right to switch off GPS, or to intro-

duce errors, for example if terrorists are thought to be using it. But so many  
 diverse systems now depend on GPS, from Google Maps to Uber, that respon-  
 sible governments are unlikely to. However there are many applications with  
 motivated opponents. Some countries use GPS to do road pricing, or to enforce  
 parole terms on released prisoners via electronic ankle tags, as I discussed in  
 section 14.4 As a result, GPS jammers appeared in car magazines in 2007 for  
 $700, and now cost under $100; they’re used by truck drivers to cheat road  
 toll systems, company car drivers who want to stop their boss knowing where  
 they’re going, and car thieves. Cheap devices have short ranges, of typically  
 5–10m.

GPS spooﬁng takes slightly more work. An example is *meaconing*, where

you sample the signals at location A and retransmit them at location B (this  
 is also known as a *wormhole attack*). The result is that anyone near B thinks  
 they’re near A instead. This is used as a defensive mechanism in the limousines  
 of some heads of government (a sophisticated assassin could use this to target  
 a missile). Some countries engage in systematic GPS jamming, an example

being Russia along its border with Norway. Spooﬁng can be largely detected  
 using differential GPS, where you use another receiver at a known location as  
 a reference point (the FAA’s trick), and with interferometric GPS, also known  
 as S-GPS, where you use the signals captured by successive readings by the  
 same receiver to produce a synthetic aperture. This also increases sensitivity  
 and deals with multipath in urban canyons, the main source of large errors in

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 716 | Ross Anderson |

*23.4. SURVEILLANCE AND TARGET ACQUISITION*

current equipment1.

In addition to the US GPS system, Russia, China and Europe have separate

navigation satellite systems using the same principles; collectively, such systems  
 are known as GNSS.

**23.4** **Surveillance and Target Acquisition**

Those aspects of electronic warfare that have to do with target acquisition and  
 weapon guidance 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 communi-  
 cations, much of the same science applies to both.)

The main methods used to detect hostile targets and guide weapons to them

are sonar, radar and infrared. The ﬁrst to be developed was sonar, which

was invented and deployed in World War 1 (under the name of ‘Asdic’), and  
 still dominates submarine warfare [846]. Elsewhere the key sensor is radar.

Although it 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 [855, 990]. The electronic attack and protection techniques

developed for it tend to be better developed than, and often go over to, systems  
 using other sensors.

**23.4.1** **Types of radar**

The wide range of deployed systems includes 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 classic textbook on the  
 technology is by Schleher [1662].

Early radar designs for search applications may have a rotating antenna

that emits a sequence of pulses and detects echos. In the days before digital  
 electronics, the sweep in the display tube could be mechanically rotated in sync  
 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 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.

1Full disclosure: the company that developed S-GPS, Focal Point Positioning, was started

by one of my postdocs and I’m an investor in it.

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 717 | Ross Anderson |

*23.4. SURVEILLANCE AND TARGET ACQUISITION*

*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.

An example of gating in a non-military application is adaptive cruise control

in cars. This uses radar, gated to ignore vehicles whose relative speed is too  
 great (so it doesn’t panic at oncoming vehicles) as well as vehicles that are too  
 near or too far. You may notice that if another car pushes in close in front  
 of you, less than 20m away, your cruise control won’t notice it and won’t slow  
 down.

**23.4.2** **Jamming techniques**

Electronic attack can be passive or active.

The earliest countermeasure to be widely used was *chaff* – thin strips of

conducting foil that are cut to 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 Doppler: as  
 chaff is very light it comes to rest almost at once and can be distinguished fairly  
 easily from moving targets.

Other techniques include small decoys with active repeaters that retransmit

radar signals and larger decoys that simply reﬂect them; sometimes one vehicle  
 (such as a helicopter) acts as a decoy for another more valuable one (such as an  
 aircraft carrier). These principles are quite general. Weapons that home in on  
 their targets using *radio direction ﬁnding* (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 forces the enemy to place their  
 air defense radars closer together, so they have 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 a low-RCS  
 aspect to identiﬁed hostile emitters (the F117 became known to its pilots as the  
 ‘wobbly goblin’).

Active countermeasures are much more diverse. Early jammers simply gen-

erated a lot of noise in the range of frequencies used by the target radar; this  
 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

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 718 | Ross Anderson |

*23.4. SURVEILLANCE AND TARGET ACQUISITION*

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 picks up a jamming signal. And jamming isn’t restricted to one  
 side; as well as being used by the target, the radar itself can also send spurious  
 signals from an auxiliary antenna to mask the real signal or to 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 hostile sig-  
 nals. Defenses against such weapons include the use of decoy transmitters,

blinking transmitters on and off, and *passive radar* – which exploits the signals  
 from existing transmitters such as TV and radio stations when they bounce off  
 targets.

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 sys-

tematic 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*. Modern equipment stores received waveforms  
 in *digital radio frequency memory* (DRFM) and manipulates them using signal  
 processing.

An elementary countermeasure is *burn-through*. By lowering the pulse repe-

tition 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 fre-

quency. Each outgoing pulse is either delayed or not depending on a *lag se-*

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 719 | Ross Anderson |

*23.4. SURVEILLANCE AND TARGET ACQUISITION*

*quence* generated by a random number generator, so the jammer cannot an-  
 ticipate 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 (counter)3-measure, is for the radar to have  
 a *leading edge tracker*, which responds only to the ﬁrst return pulse; and the  
 (counter)4-measures can include jamming at such a high power that the re-  
 ceiver’s automatic gain control circuit is captured. An alternative is *cover jam-*  
 *ming* 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 wave-  
 forms 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 transpon-  
 ders 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 CPUs are  
 powerful enough to manufacture realistic false returns.

**23.4.3** **Advanced radars and countermeasures**

A number of advanced techniques are used to defend against jamming.

*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 don’t wish the  
 target to detect you long before you detect it.

*Pulsed Doppler* is much the same as Doppler, and sends a series of phase sta-

ble 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 ad-  
 vantage 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 modern  
 variant is to excite multiple velocity gates with deceptive returns.

*Monopulse* became one of the most popular techniques. It was used, for

example, in the Exocet missiles that proved so difficult to jam in the Falklands

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 720 | Ross Anderson |

*23.4. SURVEILLANCE AND TARGET ACQUISITION*

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 powerful trick is *passive coherent location*. Lockheed’s ‘Silent Sentry’

system has no emitters at all, but rather uses reﬂections of commercial radio  
 and television broadcast signals to detect and track airborne objects [164].The  
 receivers, being passive, are hard to locate and attack; knocking out the sys-  
 tem 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 en-  
 tail steering the aircraft so that it presents the nulls in its radar cross-section  
 to visible emitters. Passive location actually goes back to the radar pioneer  
 Robert Watson-Watt in the 1930s and appears to have been ﬁrst used by the  
 Germans from 1942 when their Klein Heidelberg station exploited British Chain  
 Home radar signals to track RAF aircraft (in EW parlance, it was a ‘hitchhiker’).  
 When Britain realised this was happening in 1944, the Chain Home signals were  
 jittered [824].

One research frontier in 2020 is *cognitive radar*. Attack and defence have be-

come more complex since 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. Simon Haykin  
 and colleagues studied the strategies and tactics used by bats, who adapt their  
 sonar intelligently while hunting insects, and applied this ﬁrst to radio for the  
 efficient use of spectrum, then to radar in a seminal 2006 paper [872]. From the  
 moment a radar (or sonar) is switched on, it builds up knowledge of its environ-  
 ment, the interesting aspects of which are mostly dynamic. The basic idea is  
 that a cognitive radar does a recursive update of a model of its environment and  
 uses this to illuminate it intelligently, using learning mechanisms. This becomes  
 adversarial with non-cooperative targets. There is now vigorous research into  
 the fusion of ideas from the human visual system and neural networks more  
 generally, Bayesian target tracking and signal processing.

**23.4.4** **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 strong and stable compared with real targets.

Active infrared jamming is less widespread than radar jamming because it’s

harder; it tends to exploit features of the hostile sensor by pulsing at a rate or  
 in a pattern that causes confusion. Some infrared defense systems are starting  
 to employ lasers to disable the sensors of incoming weapons; and it’s emerged

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 721 | Ross Anderson |

*23.5. IFF SYSTEMS*

that a number of ‘UFO’ sightings have actually been due to various kinds of  
 jamming (both radar and infrared) [175].

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, used 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 17.8, combining two alarm systems will generally  
 result in improving either the false alarm or the missed alarm rate, while making  
 the other worse. If you scramble your ﬁghters when you see a blip on either the  
 radar or the infrared, you’ll have 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.

Things become more complex where the attacker’s on a platform that’s vul-

nerable to counter-attack, such as a ship or aircraft. It will have systems for  
 threat recognition, direction ﬁnding and missile approach warning, whose re-  
 ceivers will be deafened by its 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.

During the Cold War, you expected each side to 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 would 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;  
 and the move to cognitive systems has changed doctrine to “subtly disrupt  
 the enemy’s communications and radar networks without their realizing they’re  
 being deceived” [721].

**23.5** **IFF Systems**

With multiple vehicles engaged, it’s also necessary to have a reliable way of  
 distinguishing friend from foe. *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 US and allied forces.  
 Incidents in which US aircraft bombed British soldiers have contributed signiﬁ-  
 cantly 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 Judges

12:5–6 (which I quote at the head of the chapter on biometrics): the Israelites  
 identiﬁed enemy soldiers by their inability to pronounce ‘Shibboleth’. World  
 War 2 saw the French resistance asking people to pronounce ‘grenouille’, and  
 anyone who couldn’t was presumed German. In the early years of that conﬂict,  
 air identiﬁcation was procedural: allied bombers would be expected to cross  
 the coast at particular times and places, while stragglers would announce their

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 722 | Ross Anderson |

*23.5. IFF SYSTEMS*

lack of hostile intent by a pre-arranged manoeuvre such as ﬂying 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 then some early attempts at automation: when allied aircraft started  
 to carry IFF beacons, the German air defence found they could detect the planes  
 by triggering them [824].

The Korean war saw the arrival on both sides of jet aircraft and missiles,

which made it impractical to identify targets visually. Early IFF systems simply  
 used a 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.

The legacy NATO system is the Mark XII, introduced in the 1960s and

designed to solve the protocol problems discussed in section 4.3.3. The Mark  
 XII secure mode uses a 32-bit challenge and a 4-bit response. If challenges or  
 responses are too long, then the radar’s pulse repetition frequency (and thus  
 its accuracy) would be degraded. It 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 clustered near the center screen, which would  
 light up. Reﬂection attacks are prevented, and MIG-in-the-middle attacks made  
 much harder, because the challenge uses a focused antenna, while the receiver is  
 omnidirectional. (The antenna used for the challenge is typically the ﬁre control  
 radar, which in older systems was conically scanned.)

This has been largely replaced by the Mark XIIA which has a backwards-

compatible mode, but uses spread-spectrum waveforms in the new Mode 5,  
 which has been the focus of development efforts by the US services and NATO  
 armed forces during the 2010s. Such systems also have compatibility modes with  
 the systems used by civil aircraft to ‘squawk’ their ID to secondary surveillance  
 radar. However, 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

Gulf War 1 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 differ-  
 ent 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 ex-  
 tend IFF to ground troops. But when Gulf War 2 came along, nothing decent  
 had been deployed. A report from Britain’s National Audit Office describes  
 what went wrong [1389]. 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’), 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 US at one extreme and  
 Greece (for example) at the other was a near hopeless task.”

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 723 | Ross Anderson |

*23.6. IMPROVISED EXPLOSIVE DEVICES*

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. There  
 are some sexy systems used by a small number of units in Iraq that let all  
 soldiers see each other’s 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 maneuvers like driving through each  
 other’s kill zones, but are not a panacea in complex warfare such as Iraq in the  
 late 2000s and early 2010s: there, the key networks are social, not electronic, and  
 it’s hard to automate networks with nodes of unknown trustworthiness [1659].  
 The big-bang approach was tried, but failed; the Joint Tactical Radio System  
 (JTRS, pronounced ‘jitters’) set out to equip all the US services with radios that  
 interoperate and do at least two IFF modes. However, it’s one of the Pentagon’s  
 biggest procurement failures, as they spent $6bn over 15 years without delivering  
 a single usable radio [1983].

Experience has taught us that even with ‘hard-core’ IFF, where ships and

planes identify each other, the hardest issues weren’t technical but to do with  
 economics, politics and doctrine. Over two decades 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 US suppliers.

Underlying doctrinal tensions added to this. US doctrine, the ‘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 ma-  
 terial 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 since the Cold War. 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. US aircraft duly bombed  
 and killed a number of allied servicemen, which weakened the alliance. What  
 will happen now, given deglobalisation and President Trump’s impatience with  
 foreign allies, is anyone’s guess.

**23.6** **Improvised Explosive Devices**

A signiﬁcant effort was made in electronic-warfare measures to counter the im-  
 provised explosive devices (IEDs) that were the weapon of choice of insurgents in

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 724 | Ross Anderson |

*23.6. IMPROVISED EXPLOSIVE DEVICES*

Iraq and Afghanistan. The ﬁrst IED attack on U.S. forces took place in March  
 2003, and they rose to a peak of 25,000 in 2007 with over 100,000 in total.  
 These bombs became 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 can be built by hobbyists for under $1000, we are  
 starting to see improvised cruise missiles used in Syria and elsewhere, including  
 an attempt to assassinate Venezuela’s President Maduro.

Anyway, over 33,000 jammers were 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” [140]. The effect was  
 that the proportion of radio-controlled IEDs dropped from 70% to 10%, while  
 the proportion triggered by command wires increased to 40%.

Rebels have been building IEDs since at least Guy Fawkes, who tried to

blow up England’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 in the 1980s and early 1990s. 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 a total of about 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 Pakistan. Bombers can use any device that will ﬂip a switch  
 at a distance, and used 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 ra-  
 dio 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 did not translate into a reduction

in allied casualties. The IED makers simply switched from radio-controlled

bombs to devices detonated by pressure plates, command wires, passive infrared  
 or volunteers. The defence focus shifted to a mix of tactics: ‘right of boom’  
 measures such as better vehicle armor and autonomous vehicles, and ‘left of

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 725 | Ross Anderson |

*23.7. DIRECTED ENERGY WEAPONS*

boom’ measures such as disrupting the bomb-making networks. Better armor  
 had some effect: while in 2003 almost every IED caused a coalition casualty, by  
 2007 it took four devices on average [140]. Armored vehicles were also a key  
 tactic in other insurgencies, while the DARPA investment in self-driving vehicles  
 paid off a decade later in the form of a surge of work on driver assistance and  
 even autonomous road vehicles by commercial ﬁrms such as Waymo and Tesla.  
 Network disruption, though, is a longer-term play as it depends on building  
 good sources of human intelligence; Britain and Israel spent years targeting  
 bombmakers in Ireland and Lebanon respectively.

**23.7** **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 [990]. 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 deto-

nation 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  
 that matter, most electronic equipment on the US west coast, from Seattle  
 to San Diego, could be wiped out by a blast 250 miles above Salt Lake City.  
 Such an attack would kill no-one directly but could cause economic damage on  
 the scale of the coronavirus pandemic [122]. A Carrington event – a massive  
 solar ﬂare, as observed by the astronomer Richard Carrington in 1859 – would  
 cause similar disruption; that caused auroras as far south as the Caribbean.  
 Telegraph systems failed all over Europe and North America, sometimes giving  
 their operators electric shocks. Lloyd’s of London later estimated that the cost  
 of such an event to the USA alone could be in the low trillions of dollars, and that  
 such an event is inevitable every generation or two [917]. Smaller geomagnetic  
 storms happen regularly, for example in 1989 and 2003. For this reason, critical  
 military systems are carefully shielded, big IT service ﬁrms disperse their data  
 centres round the globe, we have warning satellites, and well-run utilities spend

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 726 | Ross Anderson |

*23.8. INFORMATION WARFARE*

money to protect critical assets such as large transformers.

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 transis-  
 tors 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 dam-  
 age would be to everyday electronic devices. Replacing the millions of gadgets  
 on which a city’s life depends would be extremely tiresome.

For battleﬁeld use, it’s desirable for EMP weapons to ﬁt into a standard

bomb or shell casing rather than having to be truck-mounted. Their military  
 use is however limited. The US tried a device called Blow Torch in Iraq as a  
 means of frying the electronics in IEDs, but it didn’t work well [140]. There’s  
 a survey of usable technologies at [1082] that describes how power pulses in  
 the terawatt range can be generated using explosively-pumped ﬂux compres-  
 sion generators and magnetohydrodynamic devices, as well as by high-power  
 microwave transmitters. But EMP bombs dropped from aircraft need to de-  
 ploy 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. Military command and control systems that are already hardened for  
 nuclear EMP should be unaffected.

The real signiﬁcance of EMP may be to give a blackmail weapon to countries

such as Iran and North Korea with primitive nuclear technology. When North  
 Korea ﬁres a missile into the sea near Japan, it sends a signal: “We can switch  
 off your economy any time we like, and without directly killing a single Japanese  
 civilian either.” Japan is now developing anti-missile defences. 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’.

**23.8** **Information warfare**

The phrase *Information warfare* came into use from about 1995. Its popularity  
 was boosted by operational experience in Gulf War 1. 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

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 727 | Ross Anderson |

*23.8. INFORMATION WARFARE*

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 anti-radiation 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 US  
 Army was already calling for bids for virus production [1206].) The operation  
 achieved its goal of ensuring zero allied casualties on the ﬁrst night of the aerial  
 bombardment. Military planners and think tanks started to consider how to  
 build on the success.

In April 2007, information warfare 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 dis-  
 tributed denial-of-service attacks that appeared to originate from Russia [525].  
 Estonia’s computer emergency response team tackled the problem with cool  
 professionalism, but their national leadership invoked the NATO treaty, call-  
 ing for US military help against Russia. Russia had deniability: the packet

storms were launched by Russian botnet herders, reacting to the news from  
 Estonia and egging each other on via chat rooms; the one man convicted of  
 the attacks was an ethnic Russian teenager in Estonia itself. There had 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. Nonetheless NATO  
 did respond by setting up an information warfare centre in Tallinn, and as I  
 described in section 2.2.3, one outcome was the Tallinn Manual, which sets out  
 the military and international law applicable to online operations designed to  
 have real-world effects in conﬂicts between states [1664].

States must act in self-defense or with some other lawful justiﬁcation and in

accordance with the law of armed conﬂict. Attacks are operations reasonably  
 expected to cause injury to people or damage to property; they may only be  
 directed at combatants and their logistics, not at civilians; attacks must be  
 geographically limited, not indiscriminate; and some targets are off-limits, from  
 hospitals and places of worship to nuclear power stations. Interpretation could  
 keep the lawyers busy though. Infrastructure used by both military and civilian  
 organisations is fair game, and although ‘treachery’ is prohibited, ‘ruses of war’  
 are not.

In section 2.2.3, I described how Estonia was just a warm-up for later Russian

operations in Ukraine, where the Russians took down electricity infrastructure  
 and did signiﬁcant damage to companies operating there by the NotPetya worm,  
 which inﬂicted signiﬁcant collateral damage on some international companies  
 with offices in that country.

But what’s information warfare anyway? The conventional view from the

mid-2000s, arising out of Gulf War 1, was expressed by Whitehead [1977]:

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

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 728 | Ross Anderson |

*23.8. INFORMATION WARFARE*

Cynics took the view that it was just a remarketing of the things the agencies

have been doing for decades anyway, in an attempt to maintain their budgets  
 post-Cold-War.

However the most far-sighted analyst at the time was Dorothy Denning of the

Naval Postgraduate School whose 1999 book on the topic deﬁned information  
 warfare as “operations that target or exploit information media in order to win  
 some advantage over an adversary” [539]. This was 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 [540].

A similar view of information warfare, from a writer whose background

was defense planning rather than computer security, was given by Edward  
 Waltz [1977]. He deﬁned *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 aim of such superiority is  
 to conduct 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.

**23.8.1** **Attacks on control systems**

If you want to use computer exploitation to do real damage to a rival nation,  
 perhaps the ﬁrst thing to look at is electricity generation and distribution. Tak-  
 ing down the grid is the cyber equivalent of a nuclear strike; once the electricity  
 supply fails, then pretty well everything else in a modern economy shuts down  
 too. For example, a ﬁve-week failure of the power supply to the central business  
 district of Auckland, New Zealand, in 1996 led to 60,000 of the 74,000 employees  
 having to work from home or from relocated offices, while most of the area’s  
 6,000 apartment dwellers moved out for the duration [839]. And perhaps the  
 worst terrorist ‘near miss’ in recent history was an IRA attempt in 1996 to blow  
 up transformers at the big substations that supply London [231]. This failed  
 because a senior IRA commander was a British agent; had it been successful it  
 would have wrecked electricity supplies to much of London for many months,  
 blacking out millions of people and businesses responsible for maybe a third  
 of Britain’s GDP. Finally, attacks on electricity transmission and distribution  
 have been a standard US tactic in wars from Serbia to Iraq. (In fact, the Iraq  
 insurgency after 2003 was fuelled by delays in restoring the power supply, which  
 left millions of Iraqis sweltering in the summer heat with no air conditioning.)

Security researchers started paying attention to control systems in the mid

2000s once it was noticed that the protocols used to manage assets such as  
 electricity grids and petrochemical plants, namely Modbus and DNP3, did not  
 support authentication, as these systems had evolved in a world of private net-  
 works – with ﬁxed LANs inside installations and leased lines linking them to  
 control centres. Firms started moving to IP networks from the late 1990s be-  
 cause it was cheaper, but this meant that, without authentication, anyone who  
 knew the IP address of a sensor could read it, and anyone who knew the address  
 of an actuator could operate it. After one or two accidents caused by pranks,

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 729 | Ross Anderson |

*23.8. INFORMATION WARFARE*

and an incident in 2000 where a disgruntled employee of a water company’s IT  
 contractor caused a spill of 800 tons of sewage in Maroochy, Australia [7], there  
 started to emerge a control-systems security research community.

Governments tried to help with regulation. The US Departments of En-

ergy and Homeland Security launched an initiative in 2006, and North Ameri-  
 can Electric Reliability Corporation (NERC), which sets standards for the bulk  
 power system, ruled in its Critical Infrastructure Protection (CIP) standard that  
 any generator with a black-start capability would need to have basic informa-  
 tion security compliance. Black start is the ability to start up even if the grid  
 is down; hydro power stations can do this, nuclear stations can’t, and coal-ﬁred  
 stations can generally only do a black start if they have an auxiliary diesel gen-  
 erator. The industry’s response was that some coal-ﬁred plants scrapped their  
 diesel plant, as information security could not be added to their regulated cost  
 base and therefore came off the bottom line [104].

Attempts were also made to extend control-system protocols to support en-

cryption and authentication, but this is seriously difficult. There are three main  
 vendors of electricity substations, and if one becomes the prime contractor on  
 a project it will typically buy components from the other two, so compatibility  
 is essential. Substations have a design life of typically 40 years and come with  
 maintenance contracts, so the rate of change is glacial. The threat model is  
 also interesting. Anyone who can get physical access can switch off the power  
 by pressing the red button; they can even destroy the transformer by causing  
 an internal short-circuit, which takes only one bullet. It therefore makes lit-  
 tle sense to encrypt or even just authenticate traffic on the substation LAN,  
 and doing that is hard anyway as some of the control traffic has a 4ms latency  
 requirement [731]. The only practical outcome was to secure the logical perime-  
 ter – the communications from the substation to the network control centre –  
 just as one secures the asset physically by using a cage or a building. So one  
 practical outcome of this research programme was startups whose focus was  
 to enable energy companies and other utilities to protect their networks by re-  
 perimeterising them. The specialist ﬁrewalls and gateways they designed have  
 now become mainstream products and are widely used by energy companies.

A second outcome was increased awareness of indirect threats to national

electricity supply. I described in section 14.2.4 how most European governments  
 decided to install smart meters, following lobbying from the meter industry, and  
 how we found that the proposed UK installation was insecure; it amounted to  
 putting a remotely commandable off switch in every home in Britain, and not  
 even protecting it with appropriate cryptographic authentication. GCHQ got  
 involved in the design, but even seven years later only a minority of UK smart  
 meters follow the ‘improved’ speciﬁcation. As we discussed in section 14.2.4,  
 the project has been a conspicuous failure in both ﬁnancial and energy-saving  
 terms.

A third outcome was a set of research tools. The Shodan search engine,

|  |  |  |
| --- | --- | --- |
| launched in 2009, crawls the Internet to locate and index connected devices, en-  abling researchers to see which devices are vulnerable from their software update  status; in 2011, ´Eireann Leverett used this to locate thousands of vulnerable con-  trol systems [1147]. A 2016 scan by Ariana Mirian and colleagues found some  60,000 vulnerable devices round the world, ranging from electricity substations | | |
| **Security Engineering** | 730 | Ross Anderson |

*23.8. INFORMATION WARFARE*

to HVAC in government buildings; they also used honeypots to track the actors  
 scanning for such devices, and although over half were from known security com-  
 panies, a signiﬁcant minority were in China or from shielded hosts [1321]. More  
 recently our group has been involved in developing better honeypots to detect  
 people doing scans and launching attacks on network-attached devices [1955]; by  
 deploying realistic honeypots in realistic network locations, it’s possible to pro-  
 voke hostile action [573]. Our monitoring of underground crime forums, which  
 goes back to the early days of control system security research, has detected no  
 sustained competent interest in control system hacking by criminal groups, so  
 it is reasonable to assume that the great majority of such activity is by state  
 actors or their proxies.

The burst of research into control systems security ran in parallel with state

actors’ growing awareness of the potential. It’s been reported that Idaho Na-  
 tional Labs, which was involved in the US regulatory push and hosted some of  
 the Scada security conferences at the time, helped the NSA and their Israeli  
 counterparts develop the Stuxnet worm, which damaged Iran’s uranium enrich-  
 ment capacity over the period 2008–2010; I described this in section 2.2.1.11.

Finally, as I described in section 2.2.3, 2015 saw Russia responding to a con-

ventional Ukrainian attack on power distribution in Crimea (a Ukrainian terri-  
 tory that Russia had annexed) by a cyber attack that took down 30 Ukrainian  
 substations, leaving 230,000 people in the dark for several hours [2067]. However,  
 that seems to have been a warning rather than attempt to do serious economic  
 damage, and since then there seem to have been no serious cyber attacks on  
 electricity distribution. There have been attacks on other control systems; no-  
 tably, Iran tried to hack Israeli water distribution systems in April 2020 with  
 a view to introducing toxic levels of chlorine into the rural water supply, but  
 the Israelis detected and stopped this. They retaliated the following month by  
 closing down one of the harbours at the Iranian port of Bandar Abbas, causing  
 tailbacks of trucks that stretched for miles [229].

But the main action has moved elsewhere.

**23.8.2** **Attacks on other infrastructure**

After the Stuxnet story broke there was a surge of interest among governments  
 worldwide in cyber-conﬂict. The prices paid in underground markets for ex-  
 ploitable vulnerabilities skyrocketed, and in addition to the overt markets in  
 vulnerabilites, there developed grey markets to which security researchers could  
 take their ideas for resale to cyber-arms manufacturers. In addition to vulner-  
 abilities that governments could use to exploit the PCs or phones of their foes,  
 both foreign and domestic, there emerged concern about attacks on information  
 infrastructure such as the Internet itself. The Russian attacks on Estonia in  
 2007 and Georgia in 2008 focused minds somewhat, as did an attack by Pak-  
 istan on YouTube in 2008 (Pakistan had planned to block the service only at  
 home, but the BGP attack it mounted caused a global outage), and an incident  
 in 2010 when China Telecom hijacked 15% of Internet addresses for 18 minutes,  
 which some observers interpreted as a test of a ‘cyber-nuke’.

The European Network and Information Security Agency (ENISA) commis-

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 731 | Ross Anderson |

*23.8. INFORMATION WARFARE*

sioned us to write a report on the Internet’s interconnect, which appeared in  
 2011 [1906]. I discussed the main ﬁndings in section 21.2.1 on BGP security.  
 It is certainly possible to tear up the Internet’s routing infrastructure by ad-  
 vertising lots of bogus routes; a number of incidents (including the Pakistani  
 and Chinese ones) have taught us that. It is also true that if an opponent

could take down the Internet for a few days in a developed country, the result  
 would be be chaos (and especially so since the coronavirus pandemic as even  
 more human activities have been forced online). One of the main technical re-  
 straints on such action is that most capable opponents would themselves suffer  
 tremendous harm, given that the online services used in most countries are glob-  
 alised. However, China is largely immune, because of its policy of separating  
 its infrastructure from the rest of the Internet using the Great Firewall, and  
 excluding US service providers such as Google, Facebook and Twitter in favour  
 of local champions. North Korea is even more isolated. Russia has been trying  
 to follow China, and as its service providers such as Vkontakte are much more  
 entangled with European and American infrastructure, President Putin passed  
 a law in May 2019 requiring Russian ISPs to be able to operate independently  
 of foreign Internet infrastructure by November. In December, a successful test  
 was announced, though nobody noticed anything happening; a second test, due  
 in March 2020, was apparently postponed because of the coronavirus [159]. If  
 that were to be made to work, then Russia, like China, would be in a position  
 to mount large-scale disruption attacks against the Internet in the rest of the  
 world.

**23.8.3** **Attacks on elections and political stability**

The period 2011–16 saw the emphasis in information operations shift from at-  
 tacks on infrastructure to political conﬂict. The period started with the Arab  
 Spring, which I will discuss in more detail in section 26.4.1. There, social media  
 were used to fuel an uprising against autocratic regimes across the Arab world;  
 although the Tunisians overthrew their dictator and achieved democracy, the  
 results elsewhere ranged from civil war in Syria and the Yemen to state failure  
 in Libya and crackdowns by rulers elsewhere. I described in section 2.2.4 how  
 Arab governments splashed out on surveillance technology from the west and  
 from Israel, and hired ex-NSA mercenaries, to track and harass their opponents  
 both at home and abroad.

By 2016, we’d seen substantial Russian interference in both the Brexit refer-

endum and the US presidential election. Russia has a long history of managed  
 elections. I wrote sarcastically in the ﬁrst edition in 2001: “I sincerely hope that  
 the election of Vladimir Putin as the president of Russia had nothing to do with  
 the fact that the national electoral reporting system is run by FAPSI, a Russian  
 signals intelligence agency formed in 1991 as the successor to the KGB’s 8th  
 and 16th directorates. Its head, General Starovoitov, was reported to be an old  
 KGB type; his agency reported directly to President Yeltsin, who chose Putin  
 as his successor.” [733, 1003] By the time Putin’s party was re-elected in 2007,  
 the cheating had become so blatant – with gross media bias and state employees  
 ordered to vote for the ruling party – that the international community would  
 not accept the result as free and fair.

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 732 | Ross Anderson |

*23.8. INFORMATION WARFARE*

By the 2012 election, as I noted in section 2.2.3, the Russian population was

sufficiently restive that Putin felt the need for external enemies to rally public  
 support. He invaded the Ukraine in 2014, claiming simultaneously to be defend-  
 ing it against fascists, and against gays and Jews, and annexed the Crimea –  
 bringing down international sanctions. This campaign involved ‘hybrid warfare’  
 tactics that combined ‘little green men’ – Russian soldiers in uniforms with-  
 out insignia, claimed to be Ukrainian anti-fascists – with various cyber-attacks,  
 propaganda and even an attack on Ukrainian media, reporting falsely that a  
 pro-Russian candidate had won an election. After Europe imposed sanctions on  
 Russia as a punishment for invading the Ukraine, the Kremlin became a major  
 funder of far-right groups throughout Europe, supporting the Brexit campaigns  
 in the UK and the rise of parties such as AfD in Germany. At the same time  
 as openly promoting fascist ideas – including the ideology of Ivan Ilyin at home  
 – Putin has managed to retain the sympathy of swathes of the anti-fascist left  
 in Europe too. The overall strategy since sanctions has been to disrupt and  
 weaken the USA and the EU by all available means.

The tactics used in such information warfare have a lot in common with

electronic warfare. Putin, and other authoritarian leaders, often swamp target  
 audiences, both at home and abroad, with fake news; this jamming undermines  
 trust in more reliable media – who are in turn accused of being ‘fake news’. If you  
 can’t stop your population from reading the New York Times, you just make sure  
 they don’t believe it [474]. There are bulk decoys, like chaff; after the Russians  
 shot down Malaysia Airlines’ ﬂight MH17 over Ukraine in 2014, they pushed  
 many different conspiracy theories in parallel [1593]. Many politicians use other  
 decoys to distract the press from news that could damage them; Trump has  
 used everything from the WHO to hydroxychloroquine [1710]. The equivalent  
 of deceiving IFF may be triangulation – the art of stealing a key aspect of the  
 opponent’s brand (as when Boris Johnson made the NHS central to his pitch  
 in the Brexit referendum). The equivalent of an anti-radiation missile might be  
 blocking an opponent’s website or choking off their funding. Corrupt leaders  
 accuse their opponents of corruption, while authoritarians who blame gays and  
 Jews for their country’s plight will happily accuse their opponents of fascism.

So it is a mistake to think that the security of an election is limited to

the anonymous but veriﬁable tallying of the vote itself. Just as an IED can  
 be defeated before the boom (by intelligence or jamming) or afterwards (by  
 armour), so also an election can be subverted before or after the vote. Even in  
 mature democracies, politicians are forever trying to manipulate the franchise  
 and the campaigning rules, such as campaign ﬁnance limits. For example, the  
 Russians contributed money to both the ‘Leave’ campaigns in Britain’s Brexit  
 referendum, which was illegal, and both campaigns separately broke overall  
 ﬁnance limits, for which they got ﬁned [1265]. The disclosure of these offences  
 did not lead to a rerun of the vote; it merely helped paralyse UK politics for three  
 years. The UK Prime Minister David Cameron had earlier changed franchise  
 rules to require all voters to register separately, rather than by households, to  
 cut the number of young people on the electoral roll (this should have helped  
 his Conservative party, but backﬁred in the referendum). The outcome was

much more due to discontent among voters and to blunders by complacent pro-  
 remain politicians than to enemy action, but the existence of an enemy actively  
 promoting harmful outcomes did not help. To this day, many remain supporters

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 733 | Ross Anderson |

*23.8. INFORMATION WARFARE*

do not accept the referendum result as valid – a truly wonderful outcome from  
 the Russians’ point of view.

Similar comments can be made on the US presidential election later that

year; I discuss the political scientist Yochai Benkler’s analysis of the effect on  
 that election of fake news in section 26.4.2. Again, the role played by the Rus-  
 sians was to exploit existing polarisation, throw petrol on the ﬁre where possible  
 (for example by leaking hacked emails from the Clinton camp, as discussed in  
 section 2.2.3) and to buy inﬂuence where they could [385]. Had Clinton won the  
 election, I expect evidence of hacked election systems would have emerged to  
 enable Trump to refuse to accept defeat. The fact that there are 6,000 different  
 voting systems across the USA makes the presidential ballot hard to steal out-  
 right by technical means, but exposes its credibility to challenge. An election  
 system is like an alarm; as we discussed in section 13.3, you can defeat an alarm  
 by destroying conﬁdence in it, so that alarms are ignored. The real customer  
 for an election is the losing party, and if one of the parties isn’t really prepared  
 to accept defeat, then a pretext may be all they need. Whether Trump wins or  
 loses in November 2020, we can expect an increase in polarisation among the  
 US electorate and a decline in America’s standing in the world – again, a win  
 for Russia.

China has largely refrained from interfering in other countries’ internal af-

fairs; as I described in section 2.2.2, they have long taken the view that an  
 uncensored Internet amounted to US subversion of communist party rule but  
 their posture on that front has been defensive. Their focus has been on building  
 their economic, technological and intelligence capacity while not conducting at-  
 tacks, whether disruptive or political, on other countries. This capacity building  
 has had political consequences, most notably in the US effort to prevent Huawei  
 dominating 5G infrastructure, as I discuss in sections 2.2.2 and 22.2.4. This  
 looks set to become a frontier in the new cold war that’s emerging as China  
 seeks to become the USA’s peer competitor. There are signs in 2020 though  
 of more aggressive diplomacy as China seeks to entrench its narrative around  
 coronavirus and exploit the USA’s chaotic response to the pandemic.

**23.8.4** **Doctrine**

The inclusion by Denning and Waltz of propaganda and other psychological  
 operations in information warfare back in 1999 was a minority view at the time,  
 but has been borne out by events since. It does have historical precedent. 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 – the tools may change but  
 the game remains the same.

In the intervening twenty years, the names have changed: the Pentagon

adopted ‘information warfare’ in 1998, changed it to ‘information operations’  
 in 2006 and ‘cyberspace operations’ in 2013 [1164]. There have been some

big blind spots: it wasn’t anybody’s job at the Pentagon in 2016 to worry  
 about people in St Petersburg pretending to be from Black Lives Matter [1221].  
 Meanwhile a lot of wrong ideas have been gradually discarded. It used to be

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 734 | Ross Anderson |

*23.9. SUMMARY*

said that attribution would be too hard; that’s not been borne out. Others  
 used to suggest that information warfare provided a casualty-free way to win:  
 ‘just hack the Iranian power grid and watch them sue for peace’. Yet more  
 developed countries are more exposed, and if a cyber attack targets civilians to  
 an even greater extent than the alternatives, then the attackers are likely to be  
 portrayed as war criminals. What’s more, if a NATO country is the aggressor,  
 the Tallinn manual will bolster the prosecution.

In the second edition of this book, I wondered whether cyber attacks would

ﬁnd their place in open conﬂict or in guerilla warfare. So far we’ve seen their  
 development by Russia into a component of a hybrid warfare strategy honed in  
 Georgia and the Ukraine. We’ve seen attacks on democratic mechanisms not  
 just in the UK and the USA but in Germany, France and elsewhere. Will this  
 be the future for the next ten years too, as the USA, Russia and China continue  
 to smile sweetly at the United Nations while kicking each other under the table?  
 Or are there other possibilities? We’ve seen cyber tactics being used by peaceful  
 demonstrators in the Arab spring, and by violent extremists in the Middle East,  
 mostly without success. What else is there? Or will states continue to be the  
 main actors?

**23.9** **Summary**

Electronic warfare ﬂourished during the Cold War, and developed a lot of inter-  
 esting techniques, some of which have found their way into mainstream informa-  
 tion security. After being starved of attention and money for years, it’s starting  
 to move back up the agenda as China aims to compete with the USA and the  
 Russians also modernise their armed forces. The AI revolution may change how  
 the game is played as cognitive radar and sonar, coupled with better techniques  
 for multisensor data fusion, move the advantage from the platform with the most  
 megawatts to the player with the smartest software. It is likely, though, that  
 victory will require effective coordination of physical force and subtle deception.

A decade ago, people already talked of electronic warfare becoming infor-

mation warfare. We have seen occasional use of cyber-weapons, from the 2010  
 Stuxnet attack on Iran’s uranium enrichment facilities to the Russian NotPetya  
 attack on the Ukraine. And it is easily observable that nation state actors are  
 making preparations to attack other nations’ critical national infrastructure.  
 However, the great majority of the information operations that have actually  
 been carried out in 2010–20 have been psychological operations and propaganda,  
 aimed at sowing discord, disrupting political institutions such as elections, and  
 deepening political polarisation. There are some interesting similarities between  
 the decoys, jamming and other techniques used to manipulate enemy radar, and  
 the techniques used to manipulate public opinion.

**Research Problems**

My own research group has two relevant interests. First, we’ve been looking at  
 adversarial machine learning. For example, if a missile uses a neural network

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 735 | Ross Anderson |

*23.9. SUMMARY*

to seek its target, then can we approximate that model well enough from ob-  
 servations to determine whether there’s an evasion strategy better than random  
 maneuvering [2071]? Can we design camouﬂage that takes a lot of computa-  
 tional effort to understand? Can we add keys to neural networks so that different  
 instances of them are vulnerable to different adversarial samples, thus limiting  
 an opponent’s ability to learn [1732]?

Second, via the Cambridge Cybercrime Centre, we collect large amounts of

data on spam, phish, malware, botnet command-and-control traffic, and other  
 online wickedness. We develop better honeypots for capturing attack traffic,  
 including attacks aimed at embedded systems. We license our collections of

data to over a hundred researchers worldwide. They are now starting to include  
 scrapes of underground fora for political extremism as well as for cybercrime.

**Further Reading**

The best all-round reference for the technical aspects of electronic warfare, from  
 radar through stealth to EMP weapons, is by Curtis Schleher [1662]; a good sum-  
 mary was written by Doug Richardson [1601]. The classic introduction to the  
 anti-jam properties of spread spectrum sequences is by Andrew Viterbi [1964];  
 the history of spread spectrum is ably told by Robert Scholtz [1682]; the classic  
 introduction to the mathematics of spread spectrum is by Raymond Pickholtz,  
 Donald Schilling and Lawrence Milstein [1525]; while the standard textbook is  
 by Robert Dixon [567]. The most thorough reference on communications jam-  
 ming is by Richard Poisel [1530]. Hugh Griffiths and Nicholas Willis describe  
 the electronic war between the RAF and the Luftwaffe in World War 2 [824],  
 while R. V. Jones’ overall history of British electronic warfare and scientiﬁc in-  
 telligence gives a lot of insight not just into how the technology developed but  
 also into strategic and tactical deception [990, 992]. The various protocols used  
 in industrial control systems and surveyed, and their vulnerabilities discussed,  
 by Santiago Figueroa-Lorenzo, Javier A˜norga, and Saioa Arrizabalaga in [684].  
 The inadequacy of US power grid hardening against Carrington events and EMP  
 are discussed by Matthew and Martin Weiss [2005]. For readings on informa-  
 tion operations, I’d recommend the readings I list at the end of the chapters  
 on psychology and on surveillance; for the Russian assault on democracy in the  
 U.S. and Europe, one starting point is a report to the Committee on Foreign  
 Relations of the U.S. Senate [385].

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 736 | Ross Anderson |