**Chapter 2**

**Who is the Opponent?**

**Going all the way back to early time-sharing systems we systems**

**people regarded the users, and any code they wrote, as the mortal**

**enemies of us and each other. We were like**

**the police force in a violent slum.**

– ROGER NEEDHAM

**False face must hide**

**what the false heart doth know**

– MACBETH

**2.1** **Introduction**

Ideologues may deal with the world as they would wish it to be, but engineers  
 deal with the world as it is. If you’re going to defend systems against attack,  
 you ﬁrst need to know who your enemies are.

In the early days of computing, we mostly didn’t have real enemies; while

banks and the military had to protect their systems, most other people didn’t  
 really bother. The ﬁrst computer systems were isolated, serving a single com-  
 pany or university. Students might try to hack the system to get more resources  
 and sysadmins would try to stop them, but it was mostly a game. When dial-up  
 connections started to appear, pranksters occasionally guessed passwords and  
 left joke messages, as they’d done at university. The early Internet was a friendly  
 place, inhabited by academics, engineers at tech companies, and a few hobby-  
 ists. We knew that malware was possible but almost nobody took it seriously  
 until the late 1980s when PC viruses appeared, followed by the Internet worm  
 in 1988. (Even that was a student experiment that escaped from the lab; I tell  
 the story in section 21.3.2.)

Things changed once everyone started to get online. The mid-1990s saw the

ﬁrst spam, the late 1990s brought the ﬁrst distributed denial-of-service attack,  
 and the explosion of mail-order business in the dotcom boom introduced credit  
 card fraud. To begin with, online fraud was a cottage industry; the same person

35

*2.1. INTRODUCTION*

would steal credit card numbers and use them to buy goods which he’d then  
 sell, or make up forged cards to use in a store. Things changed in the mid-2000s  
 with the emergence of underground markets. These let the bad guys specialise  
 – one gang could write malware, another could harvest bank credentials, and  
 yet others could devise ways of cashing out. This enabled them to get good at  
 their jobs, to scale up and to globalise, just as manufacturing did in the late  
 eighteenth century. The 2000s also saw the world’s governments putting in the  
 effort to ‘Master the Internet’ (as the NSA put it) – working out how to collect  
 data at scale and index it, just as Google does, to make it available to analysts.  
 It also saw the emergence of social networks, so that everyone could have a  
 home online – not just geeks with the skills to create their own handcrafted web  
 pages. And of course, once everyone is online, that includes not just the spooks  
 and the crooks but also the jerks, creeps, racists and bullies.

Over the past decade, this threat landscape has stabilised. We also know

quite a lot about it. Thanks to Ed Snowden and other whistleblowers, we know  
 a lot about the capabilities and methods of Western intelligence services; we’ve  
 also learned a lot about China, Russia and other nation-state threat actors. We  
 know a lot about cybercrime; online crime now makes up about half of all crime,  
 by volume and by value. There’s a substantial criminal infrastructure based on  
 malware and botnets with which we are constantly struggling; there’s also a large  
 ecosystem of scams. Many traditional crimes have gone online, and a typical ﬁrm  
 has to worry not just about external fraudsters but also about dishonest insiders.  
 Some ﬁrms have to worry about hostile governments, some about other ﬁrms,  
 and some about activists. Many people have to deal with online hostility, from  
 kids suffering cyber-bullying at school through harassment of elected politicians  
 to people who are stalked by former partners. And our politics may become  
 more polarised because of the dynamics of online extremism.

One of the ﬁrst things the security engineer needs to do when tackling a

new problem is to identify the likely opponents. Although you can design some  
 speciﬁc system components (such as cryptography) to resist all reasonable ad-  
 versaries, the same is much less true for a complex real-world system. You can’t  
 protect it against all possible threats and still expect it to do useful work at  
 a reasonable cost. So what sort of capabilities will the adversaries have, and  
 what motivation? How certain are you of this assessment, and how might it  
 change over the system’s lifetime? In this chapter I will classify online and

electronic threats depending on motive. First, I’ll discuss surveillance, intrusion  
 and manipulation done by governments for reasons of state, ranging from cyber-  
 intelligence to cyber-conﬂict operations. Second, I’ll deal with criminals whose  
 motive is mainly money. Third will be researchers who ﬁnd vulnerabilities for  
 fun or for money, or who report them out of social conscience – compelling ﬁrms  
 to patch their software and clean up their operations. Finally, I’ll discuss bad  
 actors whose reasons are personal and who mainly commit crimes against the  
 person, from cyber-bullies to stalkers.

The big service ﬁrms, such as Microsoft, Google and Facebook, have to worry

about all four classes of threat. Most ﬁrms and most private individuals will  
 only be concerned with some of them. But it’s important for a security engineer  
 to understand the big picture so you can help clients work out what their own  
 threat model should be, and what sort of attacks they should plan to forestall.

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 36 | Ross Anderson |

*2.2. THE SPOOKS*

**2.2** **The spooks**

Governments have a range of tools for both passive surveillance of networks and  
 active attacks on computer systems. Hundreds of ﬁrms sell equipment for wire-  
 tapping, for radio intercept, and for using various vulnerabilities to take over  
 computers, phones and other digital devices. However, there are signiﬁcant dif-  
 ferences among governments in scale, objectives and capabilities. We’ll discuss  
 four representative categories – the USA and its allies, China, Russia and the  
 Arab world – from the viewpoint of potential opponents. Even if the spooks  
 aren’t in your threat model today, the tools they use will quite often end up in  
 the hands of the crooks too, sooner or later.

**2.2.1** **The Five Eyes**

Just as everyone in a certain age range remembers where they were when John  
 Lennon was shot, everyone who’s been in our trade since 2013 remembers where  
 they were when they learned of the Snowden revelations on Friday 7th June of  
 that year.

**2.2.1.1** **Prism**

I was in a hotel in Palo Alto, California, reading the Guardian online before a  
 scheduled visit to Google where I’d been as a scientiﬁc visitor in 2011, helping  
 develop contactless payments for Android phones. The headline was ‘NSA Prism  
 program taps in to user data of Apple, Google and others’; the article, written  
 by Glenn Greenwald and Ewen MacAskill, describes a system called Prism that  
 collects the gmail and other data of users who are not US citizens or permanent  
 residents, and is carried out under an order from the FISA court [817]. After  
 breakfast I drove to the Googleplex, and found that my former colleagues were  
 just as perplexed as I was. They knew nothing about Prism. Neither did the  
 gmail team. How could such a wiretap have been built? Had an order been  
 served on Eric Schmidt, and if so how could he have implemented it without the  
 mail and security teams knowing? As the day went on, people stopped talking.

It turned out that Prism was an internal NSA codename for an access channel

that had been provided to the FBI to conduct warranted wiretaps. US law

permits US citizens to be wiretapped provided an agency convinces a court  
 to issue a warrant, based on ‘probable cause’ that they were up to no good;  
 but foreigners could be wiretapped freely. So for a foreign target like me, all  
 an NSA intelligence analyst had to do was click on a tab saying he believed I  
 was a non-US person. The inquiry would be routed automatically via the FBI  
 infrastructure and pipe my Gmail to their workstation. According to the article,  
 this program had started at Microsoft in 2007; Yahoo had fought it in court,  
 but lost, joining in late 2008; Google and Facebook had been added in 2009 and  
 Apple ﬁnally in 2012. A system that people thought was providing targeted,  
 warranted wiretaps to law enforcement was providing access at scale for foreign  
 intelligence purposes, and according to a slide deck leaked to the Guardian it

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 37 | Ross Anderson |

*2.2. THE SPOOKS*

was ‘the SIGAD1 most used in NSA reporting’.

The following day we learned that the source of the story was Edward Snow-

den, an NSA system administrator who’d decided to blow the whistle. The

story was that he’d smuggled over 50,000 classiﬁed documents out of a facility  
 in Hawaii on a memory stick and met Guardian journalists in Hong Kong [818].  
 He tried to ﬂy to Latin America on June 21st to claim asylum, but after the US  
 government cancelled his passport he got stuck in Moscow and eventually got  
 asylum in Russia instead. A consortium of newspapers coordinated a series of  
 stories describing the signals intelligence capabilities of the ‘Five Eyes’ countries  
 – the USA, the UK, Canada, Australia and New Zealand – as well as how these  
 capabilities were not just used but also abused.

The ﬁrst story based on the leaked documents had actually appeared two

days before the Prism story; it was about how the FISA court had ordered  
 Verizon to hand over all call data records (CDRs) to the NSA in February that  
 year [814]. This hadn’t got much attention from security professionals as we  
 knew the agencies did that anyway. But it certainly got the attention of lawyers  
 and politicians, as it broke during the Privacy Law Scholars’ Conference and  
 showed that US Director of National Intelligence James Clapper had lied to  
 Congress when he’d testiﬁed that the NSA collects Americans’ domestic com-  
 munications ‘only inadvertently’. And what was to follow changed everything.

**2.2.1.2** **Tempora**

On June 21st, the press ran stories about Tempora, a program to collect in-  
 telligence from international ﬁbre optic cables [1199]. This wasn’t a complete  
 surprise; the journalist Duncan Campbell had described a system called Eche-  
 lon in 1988 which tapped the Intelsat satellite network, keeping voice calls on  
 tape while making metadata available for searching so that analysts could select  
 traffic to or from phone numbers of interest [373, 374] (I’ll give more historical  
 background in section 26.2.6). Snowden gave us an update on the technology. In  
 Cornwall alone, 200 transatlantic ﬁbres were tapped and 46 could be collected  
 at any one time. As each of these carried 10Gb/s, the total data volume could  
 be as high as 21Pb a day, so the incoming data feeds undergo *massive volume*  
 *reduction*, discarding video, news and the like. Material was then selected using  
 *selectors* – not just phone numbers but more general search terms such as IP  
 addresses – and stored for 30 days in case it turns out to be of interest.

The Tempora program, like Echelon before it, has heavy UK involvement.

Britain has physical access to about a quarter of the Internet’s backbone, as  
 modern cables tend to go where phone cables used to, and they were often  
 laid between the same end stations as nineteenth-century telegraph cables. So  
 one of the UK’s major intelligence assets turns out to be the legacy of the  
 communications infrastructure it built to control its nineteenth-century empire.  
 And the asset is indeed signiﬁcant: by 2012, 300 analysts from GCHQ, and 250  
 from the NSA, were sifting through the data, using 40,000 and 31,000 selectors  
 respectively to sift 600m ‘telephone events’ each day.

1SIGINT (Signals Intelligence) Activity Designator

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 38 | Ross Anderson |

*2.2. THE SPOOKS*

**2.2.1.3** **Muscular**

One of the applications running on top of Tempora was Muscular. Revealed  
 on October 30th, this collected data as it ﬂowed between the data centres of  
 large service ﬁrms such as Yahoo and Google [2016]. Your mail may have been  
 encrypted using SSL en route to the service’s front end, but it then ﬂowed in the  
 clear between each company’s data centres. After an NSA PowerPoint slide on  
 ‘Google Cloud Exploitation’ was published in the Washington Post – see ﬁgure  
 2.1 – the companies scrambled to encrypt everything on their networks. Execu-  
 tives and engineers at cloud service ﬁrms took the smiley as a personal affront.  
 It reminded people in the industry that even if you comply with warrants, the  
 spooks will also hack you if they can. It made people outside the industry stop  
 and think: Google had accreted so much access to all our lives via search, mail,  
 maps, calendars and other services that unrestricted intelligence-service access  
 to its records (and to Facebook’s and Microsoft’s too) was a major privacy  
 breach.

Figure 2.1: Muscular – the slide

Two years later, at a meeting at Princeton which Snowden attended in the

form of a telepresence robot, he pointed out that a lot of Internet communica-  
 tions that appear to be encrypted aren’t really, as modern websites use content  
 delivery networks (CDNs) such as Akamai and Cloudﬂare; while the web traffic  
 is encrypted from the user’s laptop or phone to the CDN’s point of presence  
 at their ISP, it isn’t encrypted on the backhaul unless they pay extra – which  
 most of them don’t [86]. So the customer thinks the link is encrypted, and it’s  
 protected from casual snooping – but not from nation states or ﬁrms who can  
 read backbone traffic.

**2.2.1.4** **Special collection**

The NSA and CIA jointly operate the Special Collection Service (SCS) whose  
 most visible activity may be the plastic panels near the roofs of US and allied

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 39 | Ross Anderson |

*2.2. THE SPOOKS*

embassies worldwide; these hide antennas for hoovering up cellular communica-  
 tion (a program known as ‘Stateroom’). Beyond this, SCS implants collection  
 equipment in foreign telcos, Internet exchanges and government facilities. This  
 can involve classical spy tradecraft, from placing bugs that monitor speech or  
 electronic communications, through recruiting moles in target organisations, to  
 the covert deployment of antennas in target countries to tap internal microwave  
 links. Such techniques are not restricted to state targets: Mexican drug car-  
 tel leader ‘El Chapo’ Guzman was caught after US agents suborned his system  
 administrator.

Close-access operations include Tempest monitoring: the collection of infor-

mation leaked by the electromagnetic emissions from computer monitors and  
 other equipment, described in 19.3.2. The Snowden leaks disclose the collection  
 of computer screen data and other electromagnetic emanations from a number of  
 countries’ embassies and UN missions including those of India, Japan, Slovakia  
 and the EU.2.

**2.2.1.5** **Bullrun and Edgehill**

Special collection increasingly involves supply-chain tampering. SCS routinely  
 intercepts equipment such as routers being exported from the USA, adds surveil-  
 lance implants, repackages them with factory seals and sends them onward to  
 customers. And an extreme form of supply-chain tampering was when the NSA  
 covertly bought Crypto AG, a Swiss ﬁrm that was the main supplier of cryp-  
 tographic equipment to non-aligned countries during the Cold War; I tell the  
 story in more detail later in section 26.2.7.1.

Bullrun is the NSA codename, and Edgehill the GCHQ one, for ‘crypto

enabling’, a $100m-a-year program of tampering with supplies and suppliers  
 at all levels of the stack. This starts off with attempts to direct, or misdi-

rect, academic research3; it continued with placing trusted people on standards  
 committees, and using NIST’s inﬂuence to get weak standards adopted. One  
 spectacular incident was the Dual EC\_DRBG debacle, where NIST standardised  
 a random number generator based on elliptic curves that turned out to contain  
 an NSA backdoor. Most of the actual damage, though, was done by restrictions  
 on cryptographic key length, dovetailed with diplomatic pressure on allies to en-  
 force export controls, so that ﬁrms needing export licenses could have their arms  
 twisted to use an ‘appropriate’ standard, and was entangled with the Crypto  
 Wars (which I discuss in section 26.2.7). The result was that many of the systems  
 in use today were compelled to use weak cryptography, leading to vulnerabili-  
 ties in everything from hotel and car door locks to VPNs. In addition to that,  
 supply-chain attacks introduce covert vulnerabilities into widely-used software;  
 many nation states play this game, along with some private actors [890]. We’ll  
 see vulnerabilities that result from surveillance and cryptography policies in one

2If the NSA needs to use high-tech collection against you as they can’t get a software

implant into your computer, that may be a compliment!

3In the 1990s, when I bid to run a research program in coding theory, cryptography and

computer security at the Isaac Newton Institute at Cambridge University, a senior official  
 from GCHQ offered the institute a £50,000 donation not to go ahead, saying “There’s nothing  
 interesting happening in cryptography, and Her Majesty’s Government would like this state  
 of affairs to continue”. He was shown the door.

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 40 | Ross Anderson |

*2.2. THE SPOOKS*

chapter after another, and return in Part 3 of the book to discuss the policy  
 history in more detail.

**2.2.1.6** **Xkeyscore**

With such a vast collection of data, you need good tools to search it. The

Five Eyes search computer data using Xkeyscore, a distributed database that  
 enables an analyst to search collected data remotely and assemble the results.  
 Exposed on July 31 2013, NSA documents describe it as its “widest-reaching”  
 system for developing intelligence; it enables an analyst to search emails, SMSes,  
 chats, address book entries and browsing histories [815]. Examples in a 2008  
 training deck include “my target speaks German but is in Pakistan. How can I  
 ﬁnd him?” “Show me all the encrypted Word documents from Iran” and “Show  
 me all PGP usage in Iran”. By searching for anomalous behaviour, the analyst  
 can ﬁnd suspects and identify strong selectors (such as email addresses, phone  
 numbers or IP addresses) for more conventional collection.

Xkeyscore is a federated system, where one query scans all sites. Its compo-

nents buffer information at collection points – in 2008, 700 servers at 150 sites.  
 Some appear to be hacked systems overseas from which the NSA malware can  
 exﬁltrate data matching a submitted query. The only judicial approval required  
 is a prompt for the analyst to enter a reason why they believe that one of the  
 parties to the conversation is not resident in the USA. The volumes are such  
 that traffic data are kept for 30 days but content for only 3–5 days. Tasked items  
 are extracted and sent on to whoever requested them, and there’s a notiﬁcation  
 system (Trafficthief) for tipping off analysts when their targets do anything of  
 interest. Extraction is based either on ﬁngerprints or plugins – the latter allow  
 analysts to respond quickly with detectors for new challenges like steganography  
 and homebrew encryption.

Xkeyscore can also be used for target discovery: one of the training queries

is “Show me all the exploitable machines in country X” (machine ﬁngerprints  
 are compiled by a crawler called Mugshot). For example, it came out in 2015  
 that GCHQ and the NSA hacked the world’s leading provider of SIM cards,  
 the Franco-Dutch company Gemalto, to compromise the keys needed to in-  
 tercept (and if need be spoof) the traffic from hundreds of millions of mobile  
 phones [1658]. The hack used Xkeyscore to identify the ﬁrm’s sysadmins, who  
 were then phished; agents were also able to compromise billing servers to sup-  
 press SMS billing and authentication servers to steal keys; another technique  
 was to harvest keys in transit from Gemalto to mobile service providers. Ac-  
 cording to an interview with Snowden in 2014, Xkeyscore also lets an analyst  
 build a ﬁngerprint of any target’s online activity so that they can be followed  
 automatically round the world. The successes of this system are claimed to  
 include the capture of over 300 terrorists; in one case, Al-Qaida’s Sheikh Atiy-  
 atallah blew his cover by googling himself, his various aliases, an associate and  
 the name of his book [1658].

There’s a collection of decks on Xkeyscore with a survey by Morgan Marquis-

Boire, Glenn Greenwald and Micah Lee [1230]; a careful reading of the decks

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 41 | Ross Anderson |

*2.2. THE SPOOKS*

can be a good starting point for exploring the Snowden hoard4.

**2.2.1.7** **Longhaul**

Bulk key theft and supply-chain tampering are not the only ways to defeat  
 cryptography. The Xkeyscore training deck gives an example: “Show me all the  
 VPN startups in country X, and give me the data so I can decrypt and discover  
 the users”. VPNs appear to be easily defeated; a decryption service called

Longhaul ingests ciphertext and returns plaintext. The detailed description

of cryptanalytic techniques is held as *Extremely Compartmented Information*  
 (ECI) and is not found in the Snowden papers, but some of them talk of recent  
 breakthroughs in cryptanalysis. What might these be?

The leaks do show diligent collection of the protocol messages used to set up

VPN encryption, so some cryptographers suggested in 2015 that some variant of  
 the “Logjam attack” is feasible for a nation-state attacker against the 1024-bit  
 prime used by most VPNs and many TLS connections with Diffie-Hellman key  
 exchange [26]. Others pointed to the involvement of NSA cryptographers in  
 the relevant standard, and a protocol ﬂaw discovered later; yet others pointed  
 out that even with advances in number theory or protocol exploits, the NSA  
 has enough money to simply break 1024-bit Diffie-Hellman by brute force, and  
 this would be easily justiﬁed if many people used the same small number of  
 prime moduli – which they do [853]. I’ll discuss cryptanalysis in more detail in  
 Chapter 5.

**2.2.1.8** **Quantum**

There is a long history of attacks on protocols, which can be spoofed, replayed  
 and manipulated in various ways. (We’ll discuss this topic in detail in Chap-  
 ter 4.) The best-documented NSA attack on Internet traffic goes under the

codename of Quantum and involves the dynamic exploitation of one of the  
 communication end-points. Thus, to tap an encrypted SSL/TLS session to a  
 webmail provider, the Quantum system ﬁres a ‘shot’ that exploits the browser.  
 There are various ﬂavours; in ‘Quantuminsert’, an injected packet redirects the  
 browser to a ‘Foxacid’ attack server. Other variants attack software updates  
 and the advertising networks whose code runs in mobile phone apps [1995].

**2.2.1.9** **CNE**

Computer and Network Exploitation (CNE) is the generic NSA term for hack-  
 ing, and it can be used for more than just key theft or TLS session hijacking;  
 it can be used to acquire access to traffic too. Operation Socialist was the

GCHQ codename for a hack of Belgium’s main telco Belgacom5, in 2010–11.  
 GCHQ attackers used Xkeyscore to identify three key Belgacom technical staff,  
 then used Quantuminsert to take over their PCs when they visited sites like  
 LinkedIn. The attackers then used their sysadmin privileges to install malware

4There’s also a search engine for the collection at https://www.edwardsnowden.com.  
 5It is now called Proximus.

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 42 | Ross Anderson |

*2.2. THE SPOOKS*

on dozens of servers, including authentication servers to leverage further access,  
 billing servers so they could cover their tracks, and the company’s core Cisco  
 routers [734]. This gave them access to large quantities of mobile roaming traffic,  
 as Belgacom provides service to many foreign providers when their subscribers  
 roam in Europe. The idea that one NATO and EU member state would conduct  
 a cyber-attack on the critical infrastructure of another took many by surprise.  
 The attack also gave GCHQ access to the phone system in the European Com-  
 mission and other European institutions. Given that these institutions make  
 many of the laws for the UK and other member states, this was almost as if a  
 US state governor had got his state troopers to hack AT&T so he could wiretap  
 Congress and the White House.

Belgacom engineers started to suspect something was wrong in 2012, and

realised they’d been hacked in the spring of 2013; an anti-virus company found  
 sophisticated malware masquerading as Windows ﬁles. The story went pub-  
 lic in September 2013, and the German news magazine Der Spiegel published  
 Snowden documents showing that GCHQ was responsible. After the Belgian  
 prosecutor reported in February 2018, we learned that the attack must have  
 been authorised by then UK Foreign Secretary William Hague, but there was  
 not enough evidence to prosecute anyone; the investigation had been hampered  
 in all sorts of ways both technical and political; the software started deleting  
 itself within minutes of discovery, and institutions such as Europol (whose head  
 was British) refused to help. The Belgian minister responsible for telecomms,  
 Alexander de Croo, even suggested that Belgium’s own intelligence service might  
 have informally given the operation a green light [735]. Europol later adopted  
 a policy that it will help investigate hacks of ‘suspected criminal origin’; it has  
 nothing to say about hacks by governments.

A GCHQ slide deck on CNE explains that it’s used to support conventional

sigint both by redirecting traffic and by “enabling” (breaking) cryptography;  
 that it must always be “UK deniable”; and that it can also be used for “ef-  
 fects”, such as degrading communications or “changing users’ passwords on ex-  
 tremist website” [735]. Other papers show that the agencies frequently target  
 admins of phone companies and ISPs in the Middle East, Africa and indeed  
 worldwide – compromising a key technician is “generally the entry ticket to the  
 network” [1139]. As one phone company executive explained, “The MNOs were  
 clueless at the time about network security. Most networks were open to their  
 suppliers for remote maintenance with an ID and password and the techie in  
 China or India had no clue that their PC had been hacked”.

The hacking tools and methods used by the NSA and its allies are now fairly

well understood; some are shared with law enforcement. The Snowden papers  
 reveal an internal store where analysts can get a variety of tools; a series of  
 leaks in 2016–7 by the Shadow Brokers (thought to be Russian military intelli-  
 gence, the GRU) disclosed a number of actual NSA malware samples, used by  
 hackers at the NSA’s Tailored Access Operations team to launch attacks [238].  
 (Some of these tools were repurposed by the Russians to launch the NotPetya  
 worm and by the North Koreans in Wannacry, as I’ll discuss later.) The best  
 documentation of all is probably about a separate store of goodies used by the  
 CIA, disclosed in some detail to Wikileaks in the ‘Vault 7’ leaks in 2017. These  
 include manuals for tools that can be used to install a remote access Trojan

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 43 | Ross Anderson |

*2.2. THE SPOOKS*

on your machine, with components to geolocate it and to exﬁltrate ﬁles (in-  
 cluding SSH credentials), audio and video; a tool to jump air gaps by infecting  
 thumb drives; a tool for infecting wiﬁ routers so they’ll do man-in-the-middle  
 attacks; and even a tool for watermarking documents so a whistleblower who  
 leaks them could be tracked. Many of the tools are available not just for Win-  
 dows but also for OSX and Android; some infect ﬁrmware, making them hard  
 to remove. There are tools for hacking TVs and IoT devices too, and tools  
 to hamper forensic investigations. The Vault 7 documents are useful reading  
 if you’re curious about the speciﬁcations and manuals for modern government  
 malware [2019]. As an example of the law-enforcement use of such tools, in June  
 2020 it emerged that the French police in Lille had since 2018 installed malware  
 on thousands of Android phones running EncroChat, an encrypted messaging  
 system favoured by criminals, leading to the arrest of 800 criminal suspects in  
 France, the Netherlands, the UK and elsewhere, as well as the arrest of several  
 police officers for corruption and the seizure of several tons of drugs [1332].

**2.2.1.10** **The analyst’s viewpoint**

The intelligence analyst thus has a big bag of tools. If they’re trying to ﬁnd the  
 key people in an organisation – whether the policymakers advising on a critical  
 decision, or the lawyers involved in laundering an oligarch’s proﬁts – they can  
 use the traffic data in Xkeyscore to map contact networks. There are various  
 neat tools to help, such as ‘Cotraveler’ which ﬂags up mobile phones that have  
 traveled together. We have some insight into this process from our own research  
 into cybercrime, where we scrape tens of millions of messages from underground  
 forums and analyse them to understand crime types new and old. One might  
 describe the process as ‘adaptive message mining’. Just as you use adaptive  
 text mining when you do a web search, and constantly reﬁne your search terms  
 based on samples of what you ﬁnd, with message mining you also have metadata  
 – so you can follow threads, trace actors across forums, do clustering analysis  
 and use various other tricks to ‘ﬁnd more messages like this one’. The ability to  
 switch back and forth between the detailed view you get from reading individual  
 messages, and the statistical view you get from analysing bulk collections, is  
 extremely powerful.

Once the analyst moves from the hunting phase to the gathering phase, they

can use Prism to look at the targets’ accounts at Facebook, Google and Mi-  
 crosoft, while Xkeyscore will let them see what websites they visit. Traffic data  
 analysis gives still more: despite the growing use of encryption, the communi-  
 cations to and from a home reveal what app or device is used when and for how  
 long6. The agencies are pushing for access to end-to-end messaging systems  
 such as WhatsApp; in countries like the UK, Australia and China, legislators  
 have already authorised this, though it’s not at all clear which US companies  
 might comply (I’ll discuss policy in Chapter 26).

Given a high-value target, there’s a big bag of tools the analyst can install

on their laptop or cellphone directly. They can locate it physically, turn it

into a room bug and even use it as a remote camera. They can download

6See for example Hill and Mattu who wiretapped a modern smart home to measure

this [900].

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 44 | Ross Anderson |

*2.2. THE SPOOKS*

the target’s address book and contact history and feed that into Xkeyscore to  
 search recursively for their direct and indirect contacts. Meanwhile the analyst  
 can bug messaging apps, beating the end-to-end encryption by collecting the call  
 contents once they’ve been decrypted. They can set up an alarm to notify them  
 whenever the target sends or receives messages of interest, or changes location.  
 The coverage is pretty complete. And when it’s time for the kill, the target’s  
 phone can be used to guide a bomb or a missile. Little wonder Ed Snowden  
 insisted that journalists interviewing him put their phones in the fridge!

Finally, the analyst has also a proxy through which they can access the

Internet surreptitiously – typically a machine on a botnet. It might even be the  
 PC in your home office.

**2.2.1.11** **Offensive operations**

The Director NSA also heads the US Cyber Command, which since 2009 has  
 been one of ten uniﬁed commands of the United States Department of Defense.  
 It is responsible for offensive cyber operations, of which the one that made  
 a real difference was Stuxnet. This was a worm designed to damage Iran’s

uranium enrichment centrifuges by speeding them up and slowing them down  
 in patterns designed to cause mechanical damage, and was developed jointly by  
 the USA and Israel [325, 826]. It was technically sophisticated, using four zero-  
 day exploits and two stolen code-signing certiﬁcates to spread promiscuously  
 through Windows PCs, until it found Siemens programmable logic controllers  
 of the type used at Iran’s Natanz enrichment plant – where it would then install  
 a rootkit that would issue the destructive commands, while the PC assured  
 the operators that everything was ﬁne. It was apparently introduced using

USB drives to bridge the air gap to the Iranian systems, and came to light  
 in 2010 after copies had somehow spread to central Asia and Indonesia. Two  
 other varieties of malware (Flame and Duqu) were then discovered using similar  
 tricks and common code, performing surveillance at a number of companies in  
 the Middle East and South Asia; more recent code-analysis tools have traced  
 a lineage of malware that goes back to 2002 (Flowershop) and continued to  
 operate until 2016 (with the Equation Group tools) [2068].

Stuxnet acted as a wake-up call for other governments, which rushed to ac-

quire ‘cyber-weapons’ and develop offensive cyber *doctrine* – a set of principles  
 for what cyber warriors might do, developed with some thought given to ratio-  
 nale, strategy, tactics and legality. Oh, and the price of zero-day vulnerabilities  
 rose sharply.

**2.2.1.12** **Attack scaling**

Computer scientists know the importance of how algorithms scale, and exactly  
 the same holds for attacks. Tapping a single mobile phone is hard. You have to  
 drive around behind the suspect with radio and cryptanalysis gear in your car,  
 risk being spotted, and hope that you manage to catch the suspect’s signal as  
 they roam from one cell to another. Or you can drive behind them with a false

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 45 | Ross Anderson |

*2.2. THE SPOOKS*

base station7 and hope his phone will roam to it as the signal is louder than  
 the genuine one; but then you risk electronic detection too. Both are highly  
 skilled work and low-yield: you lose the signal maybe a quarter of the time.  
 So if you want to wiretap someone in central Paris often enough, why not just  
 wiretap everyone? Put antennas on your embassy roof, collect it all, write the  
 decrypted calls and text messages into a database, and reconstruct the sessions  
 electronically. If you want to hack everyone in France, hack the telco, perhaps  
 by subverting the equipment it uses. At each stage the capital cost goes up but  
 the marginal cost of each tap goes down. The Five Eyes strategy is essentially to  
 collect everything in the world; it might cost billions to establish and maintain  
 the infrastructure, but once it’s there you have everything.

The same applies to offensive cyber operations, which are rather like sabo-

tage. In wartime, you can send commandos to blow up an enemy radar station;  
 but if you do it more than once or twice, your lads will start to run into a  
 lot of sentries. So we scale kinetic attacks differently: by building hundreds of  
 bomber aircraft, or artillery pieces, or (nowadays) thousands of drones. So how  
 do you scale a cyber attack to take down not just one power station, but the  
 opponent’s whole power grid? The Five Eyes approach is this. Just as Google  
 keeps a copy of the Internet on a few thousand servers, with all the content and  
 links indexed, US Cyber Command keeps a copy of the Internet that indexes  
 what version of software all the machines in the world are using – the Mugshot  
 system mentioned above – so a Five Eyes cyber warrior can instantly see which  
 targets can be taken over by which exploits.

A key question for competitor states, therefore, is not just to what extent

they can create some electronic spaces that are generally off-limits to the Five  
 Eyes. It’s the extent to which they can scale up their own intelligence and

offensive capabilities rather than having to rely on America. The number of  
 scans and probes that we see online indicates that the NSA are not alone in  
 trying to build cyber weapons that scale. Not all of them might be nation

states; some might simply be arms vendors or mercenaries. This raises a host  
 of policy problems to which we’ll return in Part 3. For now we’ll continue to  
 look at capabilities.

**2.2.2** **China**

China is now the leading competitor to the USA, being second not just in terms  
 of GDP but as a technology powerhouse. The Chinese lack the NSA’s network  
 of alliances and access to global infrastructure (although they’re working hard  
 at that). Within China itself, however, they demand unrestricted access to

local data. Some US service ﬁrms used to operate there, but trouble followed.  
 After Yahoo’s systems were used to trap the dissident Wang Xiaoning in 2002,  
 Alibaba took over Yahoo’s China operation in 2005; but there was still a row  
 when Wang’s wife sued Yahoo in US courts in 2007, and showed that Yahoo had  
 misled Congress over the matter [1760]. In 2008, it emerged that the version of  
 Skype available in China had been modiﬁed so that messages were scanned for  
 sensitive keywords and, if they were found, the user’s texts were uploaded to a

7These devices are known in the USA as a Stingray and in Europe as an IMSI-catcher;

they conduct a man-in-the-middle attack of the kind we’ll discuss in detail in section 22.2.1.

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 46 | Ross Anderson |

*2.2. THE SPOOKS*

server in China [1959]. In December 2009, Google discovered a Chinese attack on  
 its corporate infrastructure, which became known as Operation Aurora; Chinese  
 agents had hacked into the Google systems used to do wiretaps for the FBI  
 (see Prism above) in order to discover which of their own agents in the USA  
 were under surveillance. Google had already suffered criticism for operating

a censored version of their search engine for Chinese users, and a few months  
 later, they pulled out of China. By this time, Facebook, Twitter and YouTube  
 had already been blocked. A Chinese strategy was emerging of total domestic  
 control, augmented by ever-more aggressive collection overseas.

From about 2002, there had been a series of hacking attacks on US and UK

defence agencies and contractors, codenamed ‘Titan Rain’ and ascribed to the  
 Chinese armed forces. According to a 2004 study by the US Foreign Military  
 Studies Office (FMSO), Chinese military doctrine sees the country in a state  
 of war with the West; we are continuing the Cold War by attacking China,  
 trying to overthrow its communist regime by exporting subversive ideas to it  
 over the Internet [1881]. Chinese leaders see US service ﬁrms, news websites  
 and anonymity tools such as Tor (which the State Department funds so that  
 Chinese and other people can defeat censorship) as being of one fabric with  
 the US surveillance satellites and aircraft that observe their military defences.  
 Yahoo and Google were thus seen as fair game, just like Lockheed Martin and  
 BAe.

Our own group’s ﬁrst contact with the Chinese came in 2008. We were asked

for help by the Dalai Lama, who had realised that the Chinese had hacked his  
 office systems in the run-up to the Beijing Olympics that year. One of my

research students, Shishir Nagaraja, happened to be in Delhi waiting for his UK  
 visa to be renewed, so he volunteered to go up to the Tibetan HQ in Dharamsala  
 and run some forensics. He found that about 35 of the 50 PCs in the office of the  
 Tibetan government in exile had been hacked; information was being siphoned  
 off to China, to IP addresses located near the three organs of Chinese state  
 security charged with different aspects of Tibetan affairs. The attackers appear  
 to have got in by sending one of the monks an email that seemed to come from  
 a colleague; when he clicked on the attached PDF, it had a JavaScript buffer  
 overﬂow that used a vulnerability in Adobe Reader to take over his machine.  
 This technique is called *phishing*, as it works by offering a lure that someone  
 bites on; when it’s aimed at a speciﬁc individual (as in this case) it’s called *spear*  
 *phishing*. They then compromised the Tibetans’ mail server, so that whenever  
 one person in the office sent a .pdf ﬁle to another, it would arrive with an  
 embedded attack. The mail server itself was in California.

This is pretty sobering, when you stop to think about it. You get an email

from a colleague sitting ten feet away, you ask him if he just sent it – and when he  
 says yes, you click on the attachment. And your machine is suddenly infected by  
 a server that you rent ten thousand miles away in a friendly country. We wrote  
 this up in a tech report on the ‘Snooping Dragon’ [1374]. After it came out, we  
 had to deal for a while with attacks on our equipment, and heckling at conference  
 talks by Chinese people who claimed we had no evidence to attribute the attacks  
 to their government. Colleagues at the Open Net Initiative in Toronto followed  
 through, and eventually found from analysis of the hacking tools’ dashboard that  
 the same espionage network had targeted 1,295 computers in 103 countries [1223]

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 47 | Ross Anderson |

*2.2. THE SPOOKS*

– ranging from the Indian embassy in Washington through Associated Press in  
 New York to the ministries of foreign affairs in Thailand, Iran and Laos.

There followed a series of further reports of Chinese state hacking, from a

complex dispute with Rio Tinto in 2009 over the price of iron ore and a hack  
 of the Melbourne International Film festival in the same year when it showed  
 a ﬁlm about a Uighur leader [1898]. In 2011, the Chinese hacked the CIA’s  
 covert communications system, after the Iranians had traced it, and executed  
 about 30 agents – though that did not become publicly known till later [578].  
 The ﬁrst ﬂashbulb moment was a leaked Pentagon report in 2013 that Chinese  
 hackers had stolen some of the secrets of the F35 joint strike ﬁghter, as well as  
 a series of other weapon systems [1379]. Meanwhile China and Hong Kong were  
 amounting for over 80% of all counterfeit goods seized at US ports. The Obama  
 administration vowed to make investigations and prosecutions in the theft of  
 trade secrets a top priority, and the following year ﬁve members of the People’s  
 Liberation Army were indicted in absentia.

The White House felt compelled to act once more after the June 2015 news

that the Chinese had hacked the Office of Personnel Management (OPM), get-  
 ting access to highly personal data on 22 million current and former federal  
 employees, ranging from ﬁngerprints to sensitive information from security clear-  
 ance interviews. Staff applying for Top Secret clearances are ordered to divulge  
 all information that could be used to blackmail them, from teenage drug use to  
 closeted gay relationships. All sexual partners in the past ﬁve years have to be  
 declared for a normal Top Secret clearance; for a Strap clearance (to deal with  
 signals intelligence material) the candidate even has to report any foreigners  
 they meet regularly at their church. So this leak affected more than just 22  
 million people. Officially, this invasive data collection is to mitigate the risk  
 that intelligence agency staff can be blackmailed. (Cynics supposed it was also  
 so that whistleblowers could be discredited.) Whatever the motives, putting all  
 such information in one place was beyond stupid; it was a real ‘database of ruin’.  
 For the Chinese to get all the compromising information on every American with  
 a sensitive government job was jaw-dropping. (Britain screwed up too; in 2008,  
 a navy officer lost a laptop containing the personal data of 600,000 people who  
 had joined the Royal Navy, or tried to [1072].) At a summit in September that  
 year, Presidents Obama and Xi agreed to refrain from computer-enabled theft  
 of intellectual property for commercial gain8. Nothing was said in public though  
 about military secrets – or the sex lives of federal agents.

The Chinese attacks of the 2000s used smart people plus simple tools; the

attacks on the Tibetans used Russian crimeware as the remote access Trojans.  
 The state also co-opted groups of ‘patriotic hackers’, or perhaps used them for  
 deniability; some analysts noted waves of na¨ıve attacks on western ﬁrms that  
 were correlated with Chinese university terms, and wondered whether students  
 had been tasked to hack as coursework. The UK police and security service  
 warned UK ﬁrms in 2007. By 2009, multiple Chinese probes had been reported  
 on US electricity ﬁrms, and by 2010, Chinese spear-phishing attacks had been

8The Chinese have kept their promise; according to US ﬁrms doing business in China, IP is

now sixth on the list of concerns, down from second in 2014 [704]. In any case, the phrase ‘IP  
 theft’ was always a simpliﬁcation, used to conﬂate the theft of classiﬁed information defence  
 contractors with the larger issue of compelled technology transfer by other ﬁrms who wanted  
 access to Chinese markets and the side-issue of counterfeiting.

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 48 | Ross Anderson |

*2.2. THE SPOOKS*

reported on government targets in the USA, Poland and Belgium [1304]. As  
 with the Tibetan attacks, these typically used crude tools and had such poor  
 operational security that it was fairly clear where they came from.

By 2020 the attacks had become more sophisticated, with a series of ad-

vanced persistent threats (APTs) tracked by threat intelligence ﬁrms. A cam-  
 paign to hack the phones of Uighurs involved multiple zero-day attacks, even  
 on iPhones, that were delivered via compromised Uighur websites [393]; this  
 targeted not only Uighurs in China but the diaspora too. China also conducts  
 industrial and commercial espionage, and Western agencies claim they exploit  
 managed service providers9. Another approach was attacking software supply  
 chains; a Chinese group variously called Wicked Panda or Barium compromised  
 software updates from computer maker Asus, a PC cleanup tool and a Korean  
 remote management tool, as well as three popular computer games, getting its  
 malware installed on millions of machines; rather than launching banking trojans  
 or ransomware, it was then used for spying [810]. Just as in GCHQ’s Operation  
 Socialist, such indirect strategies give a way to scale attacks in territory where  
 you’re not the sovereign. And China was also playing the Socialist game: it  
 came out in 2019 that someone had hacked at least ten western mobile phone  
 companies over the previous seven years and exﬁltrated call data records – and  
 that the perpetrators appeared to be the APT10 gang, linked to the Chinese  
 military [2017].

Since 2018 there has been a political row over whether Chinese ﬁrms should

be permitted to sell routers and 5g network hardware in NATO countries, with  
 the Trump administration blacklisting Huawei in May 2019. There had been  
 a previous spat over another Chinese ﬁrm, ZTE; in 2018 GCHQ warned that  
 ZTE equipment “would present risk to UK national security that could not be  
 mitigated effectively or practicably” [1475]10. President Trump banned ZTE  
 for breaking sanctions on North Korea and Iran, but relented and allowed its  
 equipment back in the USA subject to security controls11.

The security controls route had been tried with Huawei, which set up a cen-

tre in Oxfordshire in 2010 where GCHQ could study its software as a condition  
 of the company’s being allowed to sell in the UK. While the analysts did not ﬁnd  
 any backdoors, their 2019 report surfaced some scathing criticisms of Huawei’s  
 software engineering practices [931]. Huawei had copied a lot of code, couldn’t  
 patch what they didn’t understand, and no progress was being made in tackling  
 many problems despite years of promises. There was an unmanageable num-  
 ber of versions of OpenSSL, including versions that had known vulnerabilities  
 and that were not supported: 70 full copies of 4 different OpenSSL versions,  
 and 304 partial copies of 14 versions. Not only could the Chinese hack the

Huawei systems; so could anybody. Their equipment had been excluded for

9This became public in 2019 with the claim that they had hacked Wipro and used this to

compromise their customers [1093]; but it later emerged that Wipro had been hacked by a  
 crime gang operating for proﬁt.

10The only router vendor to have actually been caught with a malicious backdoor in its

code is the US company Juniper, which not only used the NSA’s Dual-EC backdoor to make  
 VPN traffic exploitable, but did it in such a clumsy way that others could exploit it too – and  
 at least one other party did so [413].

11This was done as a favour to President Xi, according to former National Security Adviser

John Bolton, who declared himself ‘appalled’ that the president would interfere in a criminal  
 prosecution [156].

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 49 | Ross Anderson |

*2.2. THE SPOOKS*

some years from UK backbone routers and from systems used for wiretapping.  
 The UK demanded “sustained evidence of improvement across multiple versions  
 and multiple product ranges” before it will put any more trust in it. A num-  
 ber of countries, including Australia and New Zealand, then banned Huawei  
 equipment outright, and in 2019 Canada arrested Huawei’s CFO (who is also  
 its founder’s daughter) following a US request to extradite her for conspiring  
 to defraud global banks about Huawei’s relationship with a company operating  
 in Iran. China retaliated by arresting two Canadians, one a diplomat on leave,  
 on spurious espionage charges, and by sentencing two others to death on drugs  
 charges. The USA hit back with a ban on US suppliers selling chips, software  
 or support to Huawei. The UK banned the purchase of their telecomms equip-  
 ment from the end of 2020 and said it would remove it from UK networks by  
 2027. Meanwhile, China is helping many less developed countries modernise  
 their networks, and this access may help them rival the Five Eyes’ scope in due  
 course. Trade policy, industrial policy and cyber-defence strategy have become  
 intertwined in a new Cold War.

Strategically, the question may not be just whether China could use Huawei

routers to wiretap other countries at scale, so much as whether they could use  
 it in time of tension to launch DDoS attacks that would break the Internet by  
 subverting BGP routing. I discuss this in more detail in the section 21.2.1. For  
 years, China’s doctrine of ‘Peaceful Rise’ meant avoiding conﬂict with other ma-  
 jor powers until they’re strong enough. The overall posture is one of largely de-  
 fensive information warfare, combining pervasive surveillance at home, a walled-  
 garden domestic Internet that is better defended against cyber-attack than any-  
 one else’s, plus considerable and growing capabilities, which are mainly used for  
 diligent intelligence-gathering in support of national strategic interests. They  
 are starting to bully other countries in various ways that sometimes involve on-  
 line operations. In 2016, during a dispute with Vietnam over some islands in  
 the South China Sea, they hacked the airport systems in Hanoi and Ho Chi  
 Minh City, displaying insulting messages and forcing manual check-in for pas-  
 sengers [1195]. In 2020, the EU has denounced China for spreading disruptive  
 fake news about the coronavirus pandemic [1577], and Australia has denounced  
 cyber-attacks that have happened since it called for an international inquiry into  
 the pandemic’s origins [935]. These information operations displayed a ﬁrst-class  
 overt and covert disinformation capability and followed previous more limited  
 campaigns in Hong Kong and Taiwan [564]. Diplomatic commentators note

that China’s trade policy, although aggressive, is no different from Japan’s in  
 the 1970s and not as aggressive as America’s; that the new Cold War is just as  
 misguided and just as likely to be wasteful and dangerous as the last one; that  
 China still upholds the international order more than it disrupts it; and that it  
 upholds it more consistently than the USA has done since WWII [704]. China’s  
 external propaganda aim is to present itself as a positive socio-economic role  
 model for the world, as it competes for access and inﬂuence and emerges as a  
 peer competitor to the USA and Europe.

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 50 | Ross Anderson |

*2.2. THE SPOOKS*

**2.2.3** **Russia**

Russia, like China, lacks America’s platform advantage and compensates with  
 hacking teams that use spear-phishing and malware. Unlike China, it takes the  
 low road, acting frequently as a spoiler, trying to disrupt the international order,  
 and sometimes beneﬁting directly via a rise in the price of oil, its main export.  
 The historian Timothy Snyder describes Putin’s rise to power and his embrace  
 of oligarchs, orthodox Christianity, homophobia and the fascist ideologue Ivan  
 Ilyin, especially since rigged elections in 2012. This leaves the Russian state in  
 need of perpetual struggle against external enemies who threaten the purity of  
 the Russian people [1798]. Its strategic posture online is different from China’s  
 in four ways. First, it’s a major centre for cybercrime; underground markets  
 ﬁrst emerged in Russia and the Ukraine in 2003–5, as we’ll discuss in the follow-  
 ing section on cybercrime. Second, although Russia is trying to become more  
 closed like China, its domestic Internet is relatively open and intertwined with  
 the West’s, including major service ﬁrms such as VK and Yandex [605]. Third,  
 Russia’s strategy of re-establishing itself as a regional power has been pursued  
 much more aggressively than China’s, with direct military interference in neigh-  
 bours such as Georgia and the Ukraine. These interventions have involved a  
 mixed strategy of cyber-attacks plus ‘little green men’ – troops without Russian  
 insignia on their uniforms – with a political strategy of denial. Fourth, Russia  
 was humiliated by the USA and Europe when the USSR collapsed in 1989, and  
 still feels encircled. Since about 2005 its goal has been to undermine the USA  
 and the EU, and to promote authoritarianism and nationalism as an alternative  
 to the rules-based international order. This has been pursued more forcefully  
 since 2013; Snyder tells the history [1798]. With Brexit, with the emergence of  
 authoritarian governments in Hungary, Turkey and Poland, and with author-  
 itarians in coalition governments in Italy, Slovakia and Austria, this strategy  
 appears to be winning.

Russian cyber-attacks came to prominence in 2007, after Estonia moved

a much-hated Soviet-era statue in Tallinn to a less prominent site, and the  
 Russians felt insulted. DDoS attacks on government offices, banks and media  
 companies forced Estonia to rate-limit its external Internet access for a few  
 weeks [692]. Russia refused to extradite the perpetrators, most of whom were  
 Russian, though one ethnic-Russian Estonian teenager was ﬁned. Sceptics said  
 that the attacks seemed the work of amateurs and worked because the Estoni-  
 ans hadn’t hardened their systems the way US service providers do. Estonia  
 nonetheless appealed to NATO for help, and one outcome was the Tallinn Man-  
 ual, which sets out the law of cyber conﬂict [1664]. I’ll discuss this in more  
 detail in the chapter on electronic and information warfare, in section 23.8. The  
 following year, after the outbreak of a brief war between Russia and Georgia,  
 Russian hackers set up a website with a list of targets in Georgia for Russian  
 patriots to attack [1990].

Estonia and Georgia were little more than warm-ups for the Ukraine. Fol-

lowing demonstrations in Maidan Square in Kiev against pro-Russian President  
 Yanukovich, and an intervention in February 2014 by Russian mercenaries who  
 shot about a hundred demonstrators, Yanukovich ﬂed. The Russians invaded  
 Ukraine on February 24th, annexing Crimea and setting up two puppet states  
 in the Donbass area of eastern Ukraine. Their tactics combined Russian spe-

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 51 | Ross Anderson |

*2.2. THE SPOOKS*

cial forces in plain uniforms, a welter of propaganda claims of an insurgency by  
 Russian-speaking Ukrainians or of Russia helping defend the population against  
 Ukrainian fascists or of defending Russian purity against homosexuals and Jews;  
 all of this coordinated with a variety of cyber-attacks. For example, in May the  
 Russians hacked the website of the Ukrainian election commission and rigged  
 it to display a message that a nationalist who’d received less than 1% of the  
 vote had won; this was spotted and blocked, but Russian media announced the  
 bogus result anyway [1798].

The following year, as the conﬂict dragged on, Russia took down 30 elec-

tricity substations on three different distribution systems within half an hour of  
 each other, leaving 230,000 people without electricity for several hours. They  
 involved multiple different attack vectors that had been implanted over a period  
 of months, and since they followed a Ukrainian attack on power distribution in  
 Crimea – and switched equipment off when they could have destroyed it instead  
 – seemed to have been intended as a warning [2067]. This attack was still tiny  
 compared with the other effects of the conﬂict, which included the shooting  
 down of a Malaysian Airlines airliner with the loss of all on board; but it was  
 the ﬁrst cyber-attack to disrupt mains electricity. Finally on June 27 2017 came  
 the NotPetya attack – by far the most damaging cyber-attack to date [813].

The NotPetya worm was initially distributed using the update service for

MeDoc, the accounting software used by the great majority of Ukrainian busi-  
 nesses. It then spread laterally in organisations across Windows ﬁle-shares using  
 the EternalBlue vulnerability, an NSA exploit with an interesting history. From  
 March 2016, a Chinese gang started using it against targets in Vietnam, Hong  
 Kong and the Philippines, perhaps as a result of ﬁnding and reverse engineering  
 it (it’s said that you don’t launch a cyberweapon; you share it). It was leaked  
 by a gang called the ‘Shadow Brokers’ in April 2017, along with other NSA  
 software that the Chinese didn’t deploy, and then used by the Russians in June.  
 The NotPetya worm used EternalBlue together with the Mimikatz tool that  
 recovers passwords from Windows memory. The worm’s payload pretended to  
 be ransomware; it encrypted the infected computer’s hard disk and demanded  
 a ransom of $300 in bitcoin. But there was no mechanism to decrypt the ﬁles  
 of computer owners who paid the ransom, so it was really a destructive service-  
 denial worm. The only way to deal with it was to re-install the operating system  
 and restore ﬁles from backup.

The NotPetya attack took down banks, telcos and even the radiation moni-

toring systems at the former Chernobyl nuclear plant. What’s more, it spread  
 from the Ukraine to international ﬁrms who had offices there. The world’s

largest container shipping company, Maersk, had to replace most of its comput-  
 ers and compensate customers for late shipments, at a cost of $300m; FedEx  
 also lost $300m, and Mondelez $100m. Mondelez’ insurers refused to pay out  
 on the ground that it was an ‘Act of War’, as the governments of the Ukraine,  
 the USA and the UK all attributed NotPetya to Russian military intelligence,  
 the GRU [1232].

2016 was marked by the Brexit referendum in the UK and the election of

President Trump in the USA, in both of which there was substantial Russian  
 interference. In the former, the main intervention was ﬁnancial support for the  
 leave campaigns, which were later found to have broken the law by spending too

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 52 | Ross Anderson |

*2.2. THE SPOOKS*

much [1265]; this was backed by intensive campaigning on social media [363]. In  
 the latter, Russian interference was denounced by President Obama during the  
 campaign, leading to renewed economic sanctions, and by the US intelligence  
 community afterwards. An inquiry by former FBI director Robert Mueller found  
 that Russia interfered very widely via the disinformation and social media cam-  
 paigns run by its Internet Research Agency ‘troll farm’, and by the GRU which  
 hacked the emails of the Democratic national and campaign committees, most  
 notably those of the Clinton campaign chair John Podesta. Some Trump asso-  
 ciates went to jail for various offences.

As I’ll discuss in section 26.4.2, it’s hard to assess the effects of such inter-

ventions. On the one hand, a report to the US Senate’s Committee on Foreign  
 Relations sets out a story of a persistent Russian policy, since Putin came to  
 power, to undermine the inﬂuence of democratic states and the rules-based in-  
 ternational order, promoting authoritarian governments of both left and right,  
 and causing trouble where it can. It notes that European countries use broad  
 defensive measures including bipartisan agreements on electoral conduct and  
 raising media literacy among voters; it recommends that these be adopted in  
 the USA as well [385]. On the other hand, Yochai Benkler cautions Democrats  
 against believing that Trump’s election was all Russia’s fault; the roots of popu-  
 lar disaffection with the political elite are much older and deeper [227]. Russia’s  
 information war with the West predates Putin; it continues the old USSR’s  
 strategy of weakening the West by fomenting conﬂict via a variety of national  
 liberation movements and terrorist groups (I discuss the information-warfare as-  
 pects in section 23.8.3). Timothy Snyder places this all in the context of modern  
 Russian history and politics [1798]; his analysis also outlines the playbook for  
 disruptive information warfare against a democracy. It’s not just about hack-  
 ing substations, but about hacking voters’ minds; about undermining trust in  
 institutions and even in facts, exploiting social media and recasting politics as  
 showbusiness. Putin is a judo player; judo’s about using an opponent’s strength  
 and momentum to trip them up.

**2.2.4** **The rest**

The rest of the world’s governments have quite a range of cyber capabilities, but  
 common themes, including the nature and source of their tools. Middle Eastern  
 governments were badly shaken by the Arab Spring uprisings, and some even  
 turned off the Internet for a while, such as Libya in April–July 2010, when  
 rebels were using Google maps to generate target ﬁles for US, UK and French  
 warplanes. Since then, Arab states have developed strategies that combine

spyware and hacking against high-proﬁle targets, through troll farms pumping  
 out abusive comments in public fora, with physical coercion.

The operations of the United Arab Emirates were described in 2019 by a

whistleblower, Lori Stroud [247]. An NSA analyst – and Ed Snowden’s former  
 boss – she was headhunted by a Maryland contractor in 2014 to work in Dubai as  
 a mercenary, but left after the UAE’s operations started to target Americans.  
 The UAE’s main technique was spear-phishing with Windows malware, but  
 their most effective tool, called Karma, enabled them to hack the iPhones of  
 foreign statesmen and local dissidents. They also targeted foreigners critical of

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 53 | Ross Anderson |

*2.2. THE SPOOKS*

the regime. In one case they social-engineered a UK grad student into installing  
 spyware on his PC on the pretext that it would make his communications hard to  
 trace. The intelligence team consisted of several dozen people, both mercenaries  
 and Emiratis, in a large villa in Dubai. The use of iPhone malware by the UAE  
 government was documented by independent observers [1219].

In 2018, the government of Saudi Arabia murdered the Washington Post

journalist Jamal Khashoggi in its consulate in Istanbul. The Post campaigned  
 to expose Saudi crown prince Mohammed bin Salman as the man who gave the  
 order, and in January 2019 the National Enquirer published a special edition  
 containing texts showing that the Post’s owner Jeff Bezos was having an affair.  
 Bezos pre-empted the Enquirer by announcing that he and his wife were di-  
 vorcing, and hired an investigator to ﬁnd the source of the leak. The Enquirer  
 had attempted to blackmail Bezos over some photos it had also obtained; it  
 wanted both him and the investigator to declare that the paper hadn’t relied  
 upon ‘any form of electronic eavesdropping or hacking in their news-gathering  
 process’. Bezos went public instead. According to the investigator, his iPhone  
 had been hacked by the Saudi Arabian government [199]; the malicious What-  
 sApp message that did the damage was sent from the phone of the Crown Prince  
 himself [1053]. The US Justice Department later charged two former Twitter  
 employees with spying, by disclosing to the Saudis personal account information  
 of people who criticised their government [1500].

An even more unpleasant example is Syria, where the industrialisation of

brutality is a third approach to scaling information collection. Malware attacks  
 on dissidents were reported from 2012, and initially used a variety of spear-  
 phishing lures. As the civil war got underway, police who were arresting suspects  
 would threaten female family members with rape on the spot unless the suspect  
 disclosed his passwords for mail and social media. They would then spear-phish  
 all his contacts while he was being taken away in the van to the torture chamber.  
 This victim-based approach to attack scaling resulted in the compromise of  
 many machines not just in Syria but in America and Europe. The campaigns  
 became steadily more sophisticated as the war evolved, with false-ﬂag attacks,  
 yet retained a brutal edge with some tools displaying beheading videos [737].

Thanks to John Scott-Railton and colleagues at Toronto, we have many fur-

ther documented examples of online surveillance, computer malware and phone  
 exploits being used to target dissidents; many in Middle Eastern and African  
 countries but also in Mexico and indeed in Hungary [1219]. The real issue here  
 is the ecosystem of companies, mostly in the USA, Europe and Israel, that sup-  
 ply hacking tools to unsavoury states. These tools range from phone malware,  
 though mass-surveillance tools you use on your own network against your own  
 dissidents, to tools that enable you to track and eavesdrop on phones overseas  
 by abusing the signaling system [488]. These tools are used by dictators to track  
 and monitor their enemies in the USA and Europe.

NGOs have made attempts to push back on this cyber arms trade. In

one case NGOs argued that the Syrian government’s ability to purchase mass-  
 surveillance equipment from the German subsidiary of a UK company should  
 be subject to export control, but the UK authorities were unwilling to block  
 it. GCHQ was determined that if there were going to be bulk surveillance de-  
 vices on President Assad’s network, they should be British devices rather than

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 54 | Ross Anderson |

*2.2. THE SPOOKS*

Ukrainian ones. (I describe this in more detail later in section 26.2.9.) So the  
 ethical issues around conventional arms sales persist in the age of cyber; indeed  
 they can be worse because these tools are used against Americans, Brits and  
 others who are sitting at home but who are unlucky enough to be on the contact  
 list of someone an unpleasant government doesn’t like. In the old days, selling  
 weapons to a far-off dictator didn’t put your own residents in harm’s way; but  
 cyber weapons can have global effects.

Having been isolated for years by sanctions, Iran has developed an indige-

nous cyber capability, drawing on local hacker forums. Like Syria, its main

focus is on intelligence operations, particularly against dissident Iranians, both  
 at home and overseas. It has also been the target of US and other attacks of  
 which the best known was Stuxnet, after which it traced the CIA’s covert com-  
 munications network and rounded up a number of agents [578]. It has launched  
 both espionage operations and attacks of its own overseas. An example of the  
 former was its hack of the Diginotar CA in the Netherlands which enabled it  
 to monitor dissidents’ Gmail; while its Shamoon malware damaged thousands  
 of PCs at Aramco, Saudi Arabia’s national oil company. The history of Ira-  
 nian cyber capabilities is told by Collin Anderson and Karim Sadjadpour [49].  
 Most recently, it attacked Israeli water treatment plants in April 2020; Israel  
 responded the following month with an attack on the Iranian port of Bandar  
 Abbas [229].

Finally, it’s worth mentioning North Korea. In 2014, after Sony Pictures

started working on a comedy about a plot to assassinate the North Korean  
 leader, a hacker group trashed much of Sony’s infrastructure, released embar-  
 rassing emails that caused its top ﬁlm executive Amy Pascal to resign, and  
 leaked some unreleased ﬁlms. This was followed by threats of terrorist attacks  
 on movie theatres if the comedy were put on general release. The company put  
 the ﬁlm on limited release, but when President Obama criticised them for giving  
 in to North Korean blackmail, they put it on full release instead.

In 2017, North Korea again came to attention after their Wannacry worm

infected over 200,000 computers worldwide, encrypting data and demanding  
 a bitcoin ransom – though like NotPetya it didn’t have a means of selective  
 decryption, so was really just a destructive worm. It used the NSA Eternal-  
 Blue vulnerability, like NotPetya, but was stopped when a malware researcher  
 discovered a kill switch. In the meantime it had disrupted production at car-  
 makers Nissan and Renault and at the Taiwanese chip foundry TSMC, and also  
 caused several hospitals in Britain’s National Health Service to close their ac-  
 cident and emergency units. In 2018, the US Department of Justice unsealed  
 an indictment of a North Korean government hacker for both incidents, and  
 also for a series of electronic bank robberies, including of $81m from the Bank  
 of Bangladesh [1653]. In 2019, North Korean agents were further blamed, in a  
 leaked United Nations report, for the theft of over $1bn from cryptocurrency  
 exchanges [346].

**2.2.5** **Attribution**

It’s often said that cyber is different, because attribution is hard. As a general  
 proposition this is untrue; anonymity online is much harder than you think.

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 55 | Ross Anderson |

*2.3. CROOKS*

Even smart people make mistakes in operational security that give them away,  
 and threat intelligence companies have compiled a lot of data that enable them  
 to attribute even false ﬂag operations with reasonable probability in many  
 cases [180]. Yet sometimes it may be true, and people still point to the Cli-  
 mategate affair. Several weeks before the 2009 Copenhagen summit on climate  
 change, someone published over a thousand emails, mostly sent to or from four  
 climate scientists at the University of East Anglia, England. Climate sceptics  
 seized on some of them, which discussed how to best present evidence of global  
 warming, as evidence of a global conspiracy. Official inquiries later established  
 that the emails had been quoted out of context, but the damage had been done.  
 People wonder whether the perpetrator could have been the Russians or the  
 Saudis or even an energy company. However one of the more convincing analy-  
 ses suggests that it was an internal leak, or even an accident; only one archive  
 ﬁle was leaked, and its ﬁlename (FOIA2009.zip) suggests it may have been pre-  
 pared for a freedom-of-information disclosure in any case. The really interesting  
 thing here may be how the emails were talked up into a conspiracy theory.

Another possible state action was the Equifax hack. The initial story was

that on 8th March 2017, Apache warned of a vulnerability in Apache Struts and  
 issued a patch; two days later, a gang started looking for vulnerable systems;  
 on May 13th, they found that Equifax’s dispute portal had not been patched,  
 and got in. The later story, in litigation, was that Equifax had used the default  
 username and password ‘admin’ for the portal [358]. Either way, the breach had  
 been preventable; the intruders found a plaintext password ﬁle giving access  
 to 51 internal database systems, and spent 76 days helping themselves to the  
 personal information of at least 145.5 million Americans before the intrusion  
 was reported on July 29th and access blocked the following day. Executives sold  
 stock before they notiﬁed the public on September 7th; Congress was outraged,  
 and the CEO Rick Smith was ﬁred. So far, so ordinary. But no criminal use has  
 been made of any of the stolen information, which led analysts at the time to  
 suspect that the perpetrator was a nation-state actor seeking personal data on  
 Americans at scale [1444]; in due course, four members of the Chinese military  
 were indicted for it [552].

In any case, the worlds of intelligence and crime have long been entangled,

and in the cyber age they seem to be getting more so. We turn to cybercrime  
 next.

**2.3** **Crooks**

Cybercrime is now about half of all crime, both by volume and by value, at least  
 in developed countries. Whether it is slightly more or less than half depends  
 on deﬁnitions (do you include tax fraud now that tax returns are ﬁled online?)  
 and on the questions you ask (do you count harassment and cyber-bullying?)  
 – but even with narrow deﬁnitions, it’s still almost half. Yet the world’s law-  
 enforcement agencies typically spend less than one percent of their budgets on  
 ﬁghting it. Until recently, police forces in most jurisdictions did their best to  
 ignore it; in the USA, it was dismissed as ‘identity theft’ and counted separately,  
 while in the UK victims were told to complain to their bank instead of the police

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 56 | Ross Anderson |

*2.3. CROOKS*

from 2005–15. The result was that as crime went online, like everything else,  
 the online component wasn’t counted and crime appeared to fall. Eventually,  
 though, the truth emerged in those countries that have started to ask about  
 fraud in regular victimisation surveys12.

Colleagues and I run the Cambridge Cybercrime Centre where we collect

and curate data for other researchers to use, ranging from spam and phish  
 through malware and botnet command-and-control traffic to collections of posts  
 to underground crime forums. This section draws on a survey we did in 2019 of  
 the costs of cybercrime and how they’ve been changing over time [91].

Computer fraud has been around since the 1960s, a notable early case being

the Equity Funding insurance company which from 1964-72 created more than  
 60,000 bogus policies which it sold to reinsurers, creating a special computer sys-  
 tem to keep track of them all. Electronic frauds against payment systems have  
 been around since the 1980s, and spam arrived when the Internet was opened to  
 all in the 1990s. Yet early scams were mostly a cottage industry, where individ-  
 uals or small groups collected credit card numbers, then forged cards to use in  
 shops, or used card numbers to get mail-order goods. Modern cybercrime can  
 probably be dated to 2003–5 when underground markets emerged that enabled  
 crooks to specialise and get good at their jobs, just as happened in the real  
 economy with the Industrial Revolution.

To make sense of cybercrime, it’s convenient to consider the shared infras-

tructure ﬁrst, and then the main types of cybercrime that are conducted for  
 proﬁt. There is a signiﬁcant overlap with the crimes committed by states that  
 we considered in the last section, and those committed by individuals against  
 other individuals that we’ll consider in the next one; but the actors’ motives are  
 a useful primary ﬁlter.

**2.3.1** **Criminal infrastructure**

Since about 2005, the emergence of underground markets has led to people spe-  
 cialising as providers of criminal infrastructure, most notably botnet herders,  
 malware writers, spam senders and cashout operators. I will discuss the tech-  
 nology in much greater detail in section 21.3; in this section my focus is on the  
 actors and the ecosystem in which they operate. Although this ecosystem con-  
 sists of perhaps a few thousand people with revenues in the tens to low hundreds  
 of millions, they impose costs of many billions on the industry and on society.  
 Now that cybercrime has been industrialised, the majority of ‘jobs’ are now in  
 boring roles such as customer support and system administration, including all  
 the tedious setup work involved in evading law enforcement takedowns [453].  
 The ‘ﬁrms’ they work for specialise; the entrepreneurs and technical specialists  
 can make real money. (What’s more, the cybercrime industry has been booming  
 during the coronavirus pandemic.)

12The USA, the UK, Australia, Belgium and France

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 57 | Ross Anderson |

*2.3. CROOKS*

**2.3.1.1** **Botnet herders**

The ﬁrst botnets – networks of compromised computers – may have been seen  
 in 1996 with an attack on the ISP Panix in New York, using compromised  
 Unix machines in hospitals to conduct a SYN ﬂood attack [368]. The next use  
 was spam, and by 2000 the Earthlink spammer sent over a million phishing  
 emails; its author was sued by Earthlink. Once cyber-criminals started to get  
 organised, there was a signiﬁcant scale-up. We started to see professionally

built and maintained botnets that could be rented out by bad guys, whether  
 spammers, phishermen or others; by 2007 the Cutwail botnet was sending over  
 50 million spams a minute from over a million infected machines [1832]. Bots  
 would initially contact a command-and-control server for instructions; these  
 would be taken down, or taken over by threat intelligence companies for use as  
 sinkholes to monitor infected machines, and to feed lists of them to ISPs and  
 corporates.

The spammers’ ﬁrst response was peer-to-peer botnets. In 2007 Storm sud-

denly grew to account for 8% of all Windows malware; it infected machines  
 mostly by malware in email attachments and had them use the eDonkey peer-  
 to-peer network to ﬁnd other infected machines. It was used not just for spam  
 but for DDoS, for pump-and-dump stock scams and for harvesting bank cre-  
 dentials. Defenders got lots of peers to join this network to harvest lists of bot  
 addresses, so the bots could be cleaned up, and by late 2008 Storm had been  
 cut to a tenth of the size. It was followed by Kelihos, a similar botnet that also  
 stole bitcoins; its creator, a Russian national, was arrested while on holiday in  
 Spain in 2017 and extradited to the USA where he pled guilty in 2018 [661].

The next criminal innovation arrived with the Conﬁcker botnet: the domain

generation algorithm (DGA). Conﬁcker was a worm that spread by exploiting  
 a Windows network service vulnerability; it generated 250 domain names every  
 day, and infected machines would try them all out in the hope that the botmaster  
 had managed to rent one of them. Defenders started out by simply buying up  
 the domains, but a later variant generated 50,000 domains a day and an industry  
 working group made agreements with registrars that these domains would simply  
 be put beyond use. By 2009 Conﬁcker had grown so large, with maybe ten  
 million machines, that it was felt to pose a threat to the largest websites and  
 perhaps even to nation states. As with Storm, its use of randomisation proved  
 to be a two-edged sword; defenders could sit on a subset of the domains and  
 harvest feeds of infected machines. By 2015 the number of infected machines  
 had fallen to under a million.

Regardless of whether something can be done to take out the command-

and-control system, whether by arresting the botmaster or by technical tricks,  
 the universal ﬁx for botnet infections is to clean up infected machines. But  
 this raises many issues of scale and incentives. While AV companies make tools  
 available, and Microsoft supplies patches, many people don’t use them. So long  
 as your infected PC is merely sending occasional spam but works well enough  
 otherwise, why should you go to the trouble of doing anything? But bandwidth  
 costs ISPs money, so the next step was that some ISPs, particularly the cable  
 companies like Comcast, would identify infected machines and conﬁne their  
 users to a ‘walled garden’ until they promised to clean up. By 2019 that has

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 58 | Ross Anderson |

*2.3. CROOKS*

become less common as people now have all sorts of devices on their wiﬁ, many  
 of which have no user interface; communicating with human users has become  
 harder.

In 2020, we ﬁnd many botnets with a few tens of thousands of machines that

are too small for most defenders to care about, plus some large ones that tend  
 to be multilayer – typically with peer-to-peer mechanisms at the bottom that  
 enable the footsoldier bots to communicate with a few control nodes, which in  
 turn use a domain generation algorithm to ﬁnd the botmaster. Fragmenting  
 the footsoldiers into a number of small botnets makes it hard for defenders to  
 inﬁltrate all of them, while the control nodes may be located in places that are  
 hard for defenders to get at. The big money for such botnets in 2020 appears  
 to be in clickfraud.

The latest innovation – since October 2016 – is Mirai, a family of botnets

that exploit IoT devices. The ﬁrst Mirai worm infected CCTV cameras that had  
 been manufactured by Xiaomi and that had a known factory default password  
 that couldn’t be changed. Mirai botnets scan the Internet’s IPv4 address space  
 for other vulnerable devices which typically get infected within minutes of being  
 powered up. The ﬁrst attack was on DynDNS and took down Twitter for six  
 hours on the US eastern seaboard. Since then there have been over a thousand  
 variants, which researchers study to determine what’s changed and to work out  
 what countermeasures might be used.

At any one time, there may be half a dozen large botnet herders. The Mirai

operators, for example, seem to be two or three groups that might have involved  
 a few dozen people.

**2.3.1.2** **Malware devs**

In addition to the several hundred software engineers who write malware for the  
 world’s intelligence agencies and their contractors, there may be hundreds of  
 people writing malware for the criminal market; nobody really knows (though  
 we can monitor traffic on hacker forums to guess the order of magnitude).

Within this community there are specialists. Some concentrate on turning

vulnerabilities into exploits, a nontrivial task for modern operating systems that  
 use stack canaries, ASLR and other techniques we’ll discuss later in section 6.4.1.  
 Others specialise in the remote access Trojans that the exploits install; others  
 build the peer-to-peer and DGA software for resilient command-and-control  
 communications; yet others design specialised payloads for bank fraud. The  
 highest-value operations seem to be platforms that are maintained with constant  
 upgrades to cope with the latest countermeasures from the anti-virus companies.  
 Within each specialist market segment there are typically a handful of operators,  
 so that when we arrest one of them it makes a difference for a while. Some of  
 the providers are based in jurisdictions that don’t extradite their nationals, like  
 Russia, and Russian crimeware is used not just by Russian state actors but by  
 others too.

As Android has taken over from Windows as the most frequently used oper-

ating system we’ve seen a rise in Android malware. In China and in countries  
 with a lot of second-hand and older phones, this may be software that uses an

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 59 | Ross Anderson |

*2.3. CROOKS*

unpatched vulnerability to root an Android phone; the USA and Europe have  
 lots of unpatched phones (as many OEMs stop offering patches once a phone is  
 no longer on sale) but it’s often just apps that do bad things, such as stealing  
 SMSes used to authenticate banking transactions.

**2.3.1.3** **Spam senders**

Spamming arrived on a small scale when the Internet opened to the public in the  
 mid-1990s, and by 2000 we saw the Earthlink spammer making millions from  
 sending phishing lures. By 2010 spam was costing the world’s ISPs and tech  
 companies about $1bn a year in countermeasures, but it earned its operators  
 perhaps one percent of that. The main beneﬁciaries may have been webmail  
 services such as Yahoo, Hotmail and Gmail, which can operate better spam  
 ﬁlters because of scale; during the 2010s, hundreds of millions of people switched  
 to using their services.

Spam is now a highly specialised business, as getting past modern spam ﬁlters

requires a whole toolbox of constantly-changing tricks. If you want to use spam  
 to install ransomware, you’re better off paying an existing service than trying to  
 learn it all from scratch. Some spam involves industrial-scale email compromise,  
 which can be expensive for the victim; some $350m was knocked off the $4.8bn  
 price at which Yahoo was sold to Verizon after a bulk compromise [771].

**2.3.1.4** **Bulk account compromise**

Some botnets are constantly trying to break into email and other online accounts  
 by trying to guess passwords and password recovery questions. A large email  
 service provider might be recovering several tens of thousands of accounts every  
 day. There are peaks, typically when hackers compromise millions of email

addresses and passwords at one website and then try them out at all the others.  
 In 2019, this *credential stuffing* still accounts for the largest number of attempted  
 account compromises by volume [1882]. Compromised accounts are sold on to  
 people who exploit them in various ways. Primary email accounts often have  
 recovery information for other accounts, including bank accounts if the attacker  
 is lucky. They can also be used for scams such as the stranded traveler, where  
 the victim emails all their friends saying they’ve been robbed in some foreign  
 city and asking for urgent ﬁnancial help to pay the hotel bill. If all else fails,  
 compromised email accounts can be used to send spam.

A variant on the theme is the pay-per-install service, which implants malware

on phones or PCs to order and at scale. This can involve a range of phishing  
 lures in a variety of contexts, from free porn sites that ask you to install a special  
 viewer, to sports paraphernalia offers and news about topical events. It can also  
 use more technical means such as drive-by downloads. Such services are often  
 offered by botnets which need them to maintain their own numbers; they might  
 charge third party customers $10-15 per thousand machines infected in the USA  
 and Europe, and perhaps $3 for Asia.

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 60 | Ross Anderson |

*2.3. CROOKS*

**2.3.1.5** **Targeted attackers**

We’ve seen the emergence of hack-for-hire operators who will try to compromise  
 a speciﬁc target account for a fee, of typically $750 [1882]. They will investi-  
 gate the target, make multiple spear-phishing attempts, try password recovery  
 procedures, and see if they can break in through related accounts. This contin-  
 ues a tradition of private eyes who traditionally helped in divorce cases and also  
 stalked celebrities on behalf of red-top newspapers – though with even fewer eth-  
 ical constraints now that services can be purchased anonymously online. John  
 Scott-Railton and colleagues exposed the workings of Dark Basin, a hack-for-  
 hire company that had targeted critics of ExxonMobil, and also net neutrality  
 advocates, and traced it to a company in India [1692].

In recent years, targeted attacks have also been used at scale against small

business owners and the ﬁnance staff of larger ﬁrms in order to carry out various  
 kinds of payment fraud, as I’ll discuss below in 2.3.2.

**2.3.1.6** **Cashout gangs**

Back in the twentieth century, people who stole credit card numbers would have  
 to go to the trouble of shopping for goods and then selling them to get money  
 out. Nowadays there are specialists who buy compromised bank credentials on  
 underground markets and exploit them. The prices reveal where the real value  
 lies in the criminal chain; a combination of credit card number and expiry date  
 sells for under a dollar, and to get into the single dollars you need a CVV, the  
 cardholder’s name and address, and more.

Cashout techniques change every few years, as paths are discovered through

the world’s money-laundering controls, and the regulations get tweaked to block  
 them. Some cashout ﬁrms organise armies of *mules* to whom they transfer some  
 of the risk. Back in the mid-2000s, mules could be drug users who would go to  
 stores and buy goods with stolen credit cards; then there was a period when  
 unwitting mules were recruited by ads promising large earnings to ‘agents’ to  
 represent foreign companies but who were used to remit stolen funds through  
 their personal bank accounts. The laundrymen next used Russian banks in

Latvia, to which Russian mules would turn up to withdraw cash. Then Liberty  
 Reserve, an unlicensed digital currency based in Costa Rica, was all the rage  
 until it was closed down and its founder arrested in 2013. Bitcoin took over  
 for a while but its popularity with the cybercrime community tailed off as its  
 price became more volatile, as the US Department of the Treasury started arm-  
 twisting bitcoin exchanges into identifying their customers.

As with spam, cashout is a constantly evolving attack-defence game. We

monitor it and analyse the trends using CrimeBB, a database we’ve assembled  
 of tens of millions of posts in underground hacker forums where cybercriminals  
 buy and sell services including cashout [1499]. It also appears to favour gangs  
 who can scale up, until they get big enough to attract serious law-enforcement  
 attention: in 2020, one Sergey Medvedev pleaded guilty to inﬂicting more than  
 $568 million in actual losses over the period 2010–15 [1928].

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 61 | Ross Anderson |

*2.3. CROOKS*

**2.3.1.7** **Ransomware**

One reason for the decline in cryptocurrency may have been the growth of  
 ransomware, and as the gangs involved in this switched to payment methods  
 that are easier for victims to use. By 2016–17, 42% of ransomware encountered  
 by US victims demanded prepaid vouchers such as Amazon gift cards; 14%  
 demanded wire transfers and only 12% demanded cryptocurrency; a lot of the  
 low-end ransomware aimed at consumers is now really scareware as it doesn’t  
 actually encrypt ﬁles at all [1742]. Since 2017, we’ve seen ransomware-as-a-

service platforms; the operators who use these platforms are often amateurs  
 and can’t decrypt even if you’re willing to pay.

Meanwhile a number of more professional gangs penetrate systems, install

ransomware, wait until several days or weeks of backup data have been encrypted  
 and demand substantial sums of bitcoin. This has grown rapidly over 2019–20,  
 with the most high-proﬁle ransomware victims in the USA being public-sector  
 bodies; several hundred local government bodies and a handful of hospitals  
 have suffered service failures [358]. During the pandemic, more hospitals have  
 been targeted; the medical school at UCSF paid over $1m [1480]. It’s an in-  
 ternational phenomenon, though, and many private-sector ﬁrms fall victim too.  
 Ransomware operators have also been threatening large-scale leaks of personal  
 data to bully victims into paying.

**2.3.2** **Attacks on banking and payment systems**

Attacks on card payment systems started with lost and stolen cards, with forgery  
 at scale arriving in the 1980s; the dotcom boom ramped things up further in  
 the 1990s as many businesses started selling online with little idea of how to  
 detect fraud; and it was card fraud that spawned underground markets in the  
 mid-2000s as criminals sought ways to buy and sell stolen card numbers as well  
 as related equipment and services.

Another signiﬁcant component is pre-issue fraud, known in the USA as *‘iden-*

*tity theft’* [670], where criminals obtain credit cards, loans and other assets in  
 your name and leave you to sort out the mess. I write ‘identity theft’ in paren-  
 theses as it’s really just the old-fashioned offence of impersonation. Back in the  
 twentieth century, if someone went to a bank, pretended to be me, borrowed  
 money from them and vanished, then that was the bank’s problem, not mine. In  
 the early twenty-ﬁrst, banks took to claiming that it’s your identity that’s been  
 stolen rather than their money [1727]. There is less of that liability dumping  
 now, but the FBI still records much cybercrime as ‘identity theft’ which helps  
 keep it out of the mainstream US crime statistics.

The card fraud ecosystem is now fairly stable. Surveys in 2011 and 2019

show that while card fraud doubled over the decade, the loss fell slightly as  
 a percentage of transaction value [90, 91]; the system has been getting more  
 efficient as it grows. Many card numbers are harvested in hacking attacks on  
 retailers, which can be very expensive for them once they’ve paid to notify  
 affected customers and reimburse banks for reissued cards. As with the criminal  
 infrastructure, the total costs may be easily two orders of magnitude greater  
 than anything the criminals actually get away with.

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 62 | Ross Anderson |

*2.3. CROOKS*

Attacks on online banking ramped up in 2005 with the arrival of large-scale

phishing attacks; emails that seemed to come from banks drove customers to  
 imitation bank websites that stole their passwords. The banks responded with  
 techniques such as two-factor authentication, or the low-cost substitute of asking  
 for only a few letters of the password at a time; the crooks’ response, from about  
 2009, has been credential-stealing malware. Zeus and later Trojans lurk on a  
 PC until the user logs on to a bank whose website they recognise; they then  
 make payments to mule accounts and hide their activity from the user – the  
 so-called ‘man-in-the-browser attack’. (Some Trojans even connect in real time  
 to a human operator.) The crooks behind the Zeus and later the Dridex banking  
 malware were named and indicted by US investigators in December 2019, and  
 accused of stealing some $100m, but they remain at liberty in Russia [795].  
 Other gangs have been broken up and people arrested for such scams, which  
 continue to net in the hundreds of millions to low billions a year worldwide.

Firms also have to pay attention to business email compromise, where a

crook compromises a business email account and tells a customer that their  
 bank account number has changed; or where the crook impersonates the CEO  
 and orders a ﬁnancial controller to make a payment; and social engineering  
 attacks by people pretending to be from your bank who talk you into releasing  
 a code to authorise a payment. Most targeted attacks on company payment  
 systems can in theory be prevented by the control procedures that most large  
 ﬁrms already have, and so the typical target is a badly-run large ﬁrm, or a  
 medium-sized ﬁrm with enough money to be worth stealing but not enough  
 control to lock everything down.

I’ll discuss the technicalities of such frauds in Chapter 12, along with a grow-

ing number of crimes that directly affect only banks, their regulators and their  
 retail customers. I’ll also discuss cryptocurrencies, which facilitate cybercrimes  
 from ransomware to stock frauds, in Chapter 20.

**2.3.3** **Sectoral cybercrime ecosystems**

A number of sectors other than banking have their own established cybercrime  
 scenes. One example is travel fraud. There’s a whole ecosystem of people who  
 sell fraudulently obtained air tickets, which are sometimes simply bought with  
 stolen credit card numbers, sometimes obtained directly by manipulating or  
 hacking the systems of travel agents or airlines, sometimes booked by corrupt  
 staff at these ﬁrms, and sometimes scammed from the public directly by stealing  
 their air miles. The resulting cut-price tickets are sold directly using spam or  
 through various affiliate marketing scams. Some of the passengers who use them  
 to ﬂy know they’re dubious, while others are dupes – which makes it hard to deal  
 with the problem just by arresting people at the boarding gate. (The scammers  
 also supply tickets at the last minute, so that the alarms are usually too late.)  
 For an account and analysis of travel fraud, see Hutchings [936]. An increasing  
 number of other business sectors are acquiring their own dark side, and I will  
 touch on some of them in later chapters.

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 63 | Ross Anderson |

*2.3. CROOKS*

**2.3.4** **Internal attacks**

Fraud by insiders has been an issue since businesses started hiring people. Em-  
 ployees cheat the ﬁrm, partners cheat each other, and ﬁrms cheat their share-  
 holders. The main defence is bookkeeping. The invention of double-entry book-  
 keeping, of which our earliest records are from the Cairo of a thousand years  
 ago, enabled businesses to scale up beyond the family that owned them. This  
 whole ecosystem is evolving as technology does, and its design is driven by the  
 Big Four accounting ﬁrms who make demands on their audit clients that in  
 turn drive the development of accounting software and the supporting security  
 mechanisms. I discuss all this at length in Chapter 12. There are also inside  
 attacks involving whistleblowing, which I discuss below.

**2.3.5** **CEO crimes**

Companies attack each other, and their customers too. From the 1990s, printer  
 vendors have used cryptography to lock their customers in to using proprietary  
 ink cartridges, as I describe in section 24.6, while companies selling reﬁlls have  
 been breaking the crypto. Games console makers have been playing exactly  
 the same game with aftermarket vendors. The use of cryptography for acces-  
 sory control is now pervasive, being found even on water ﬁlter cartridges in  
 fridges [1071]. Many customers ﬁnd this annoying and try to circumvent the  
 controls. The US courts decided in the Lexmark v SCC case that this was ﬁne:  
 the printer vendor Lexmark sued SCC, a company that sold clones of its security  
 chips to independent ink vendors, but lost. So the incumbent can now hire the  
 best cryptographers they can ﬁnd to lock their products, while the challenger  
 can hire the best cryptanalysts they can ﬁnd to unlock them – and customers  
 can hack them any way they can. Here, the conﬂict is legal and open. As

with state actors, corporates sometimes assemble teams with multiple PhDs,  
 millions of dollars in funding, and capital assets such as electron microscopes13.  
 We discuss this in greater detail later in section 24.6.

Not all corporate attacks are conducted as openly. Perhaps the best-known

covert hack was by Volkswagen on the EU and US emissions testing schemes;  
 diesel engines sold in cars were programmed to run cleanly if they detected the  
 standard emission test conditions, and efficiently otherwise. For this, the CEO  
 of VW was ﬁred and indicted in the USA (to which Germany won’t extradite  
 him), while the CEO of Audi was ﬁred and jailed in Germany [1084]. VW

has set aside e25bn to cover criminal and civil ﬁnes and compensation. Other  
 carmakers were cheating too; Daimler was ﬁned e860m in Europe in 2019 [1466],  
 and in 2020 reached a US settlement consisting of a ﬁne of $1.5bn from four  
 government agencies plus a class action of $700m [1856]. Settlements for other  
 manufacturers and other countries are in the pipeline.

Sometimes products are designed to break whole classes of protection system,

an example being the overlay SIM cards described later in Chapter 12. These  
 are SIM cards with two sides and only 160 microns thick, which you stick on  
 top of the SIM card in your phone to provide a second root of trust; they were

13Full disclosure: both our hardware lab and our NGO activities have on occasion received

funding from such actors.

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 64 | Ross Anderson |

*2.3. CROOKS*

designed to enable people in China to defeat the high roaming charges of the  
 early 2010s. The overlay SIM essentially does a man-in-the-middle attack on  
 the real SIM, and can be programmed in Javacard. A side-effect is that such  
 SIMs make it really easy to do some types of bank fraud.

So when putting together the threat model for your system, stop and think

what capable motivated opponents you might have among your competitors, or  
 among ﬁrms competing with suppliers on which products you depend. The obvi-  
 ous attacks include industrial espionage, but nowadays it’s much more complex  
 than that.

**2.3.6** **Whistleblowers**

Intelligence agencies, and secretive ﬁrms, can get obsessive about ‘the insider  
 threat’. But in 2018, Barclays Bank’s CEO was ﬁned £642,000 and ordered  
 to repay £500,000 of his bonus for attempting to trace a whistleblower in the  
 bank [698]. So let’s turn it round and look at it from the other perspective –  
 that of the whistleblower. Many are trying to do the right thing, often at a fairly  
 mundane level such as reporting a manager who’s getting bribes from suppliers  
 or who is sexually harassing staff. In regulated industries such as banking they  
 may have a legal duty to report wrongdoing and legal immunity against claims  
 of breach of conﬁdence by their employer. Even then, they often lose because  
 of the power imbalance; they get ﬁred and the problem goes on. Many security  
 engineers think the right countermeasure to leakers is technical, such as data loss  
 prevention systems, but robust mechanisms for staff to report wrongdoing are  
 usually more important. Some organisations, such as banks, police forces and  
 online services, have mechanisms for reporting crimes by staff but no effective  
 process for raising ethical concerns about management decisions14.

But even basic whistleblowing mechanisms are often an afterthought; they

typically lead the complainant to HR rather than to the board’s audit com-  
 mittee. External mechanisms may be little better. One big service ﬁrm ran  
 a “Whistle-blowing hotline” for its clients in 2019; but the web page code has  
 trackers from LinkedIn, Facebook and Google, who could thus identify unhappy  
 staff members, and also JavaScript from CDNs, littered with cookies and refer-  
 rers from yet more IT companies. No technically savvy leaker would use such  
 a service. At the top end of the ecosystem, some newspapers offer ways for  
 whistleblowers to make contact using encrypted email. But the mechanisms

tend to be clunky and the web pages that promote them do not always educate  
 potential leakers about either the surveillance risks, or the operational security  
 measures that might counter them. I discuss the usability and support issues  
 around whistleblowing in more detail in Chapter 25.

This is mostly a policy problem rather than a technical one. It’s difficult

to design a technical mechanism whereby honest staff can blow the whistle on  
 abuses that have become ingrained in an organisation’s culture, such as pervasive  
 sexual harassment or ﬁnancial misconduct. In most cases, it’s immediately clear  
 who the whistleblower is, so the critical factor is whether the whistleblower will

14Google staff ended up going on strike in 2018 about the handling of sexual harassment

scandals.

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 65 | Ross Anderson |

*2.4. GEEKS*

get external support. For example, will they ever get another job? This isn’t  
 just a matter of formal legal protection but also of culture. For example, the  
 rape conviction of Harvey Weinstein empowered many women to protest about  
 sexual harassment and discrimination; hopefully the Black Lives Matter protests  
 will similarly empower people of colour [31].

An example where anonymity did help, though, was the UK parliamentary

expenses scandal of 2008–9. During a long court case about whether the public  
 could get access to the expense claims of members of parliament, someone went  
 to the PC where the records were kept, copied them to a DVD and sold the lot  
 to the Daily Telegraph. The paper published the juicy bits in instalments all  
 through May and June, when MPs gave up and published the lot on Parliament’s  
 website. Half-a-dozen ministers resigned; seven MPs and peers went to prison;  
 dozens of MPs stood down or lost their seats at the following election; and there  
 was both mirth and outrage at some of the things charged to the taxpayer. The  
 whistleblower may have technically committed a crime, but their action was  
 clearly in the public interest; now all parliamentary expenses are public, as they  
 should have been all along. If a nation’s lawmakers have their hands in the till,  
 what else will clean up the system?

Even in the case of Ed Snowden, there should have been a robust way for

him to report unlawful conduct by the NSA to the appropriate arm of gov-  
 ernment, probably a Congressional committee. But he knew that a previous  
 whistleblower, Bill Binney, had been arrested and harassed after trying to do  
 that. In hindsight, that aggressive approach was unwise, as President Obama’s  
 NSA review group eventually conceded. At the less exalted level of a commer-  
 cial ﬁrm, if one of your staff is stealing your money, and another wants to tell  
 you about it, you’d better make that work.

**2.4** **Geeks**

Our third category of attacker are the people like me – researchers who inves-  
 tigate vulnerabilities and report them so they can be ﬁxed. Academics look  
 for new attacks out of curiosity, and get rewarded with professional acclaim –  
 which can lead to promotion for professors and jobs for the students who help us.  
 Researchers working for security companies also look for newsworthy exploits;  
 publicity at conferences such as Black Hat can win new customers. Hobby hack-  
 ers break into stuff as a challenge, just as people climb mountains or play chess;  
 hacktivists do it to annoy companies they consider to be wicked. Whether on  
 the right side of the law or not, we tend to be curious introverts who need to feel  
 in control, but accept challenges and look for the ‘rush’. Our reward is often  
 fame – whether via academic publications, by winning customers for a security  
 consulting business, by winning medals from academic societies or government  
 agencies, or even on social media. Sometimes we break stuff out of irritation,  
 so we can circumvent something that stops us ﬁxing something we own; and  
 sometimes there’s an element of altruism. For example, people have come to us  
 in the past complaining that their bank cards had been stolen and used to buy  
 stuff, and the banks wouldn’t give them a refund, saying their PIN must have  
 been used, when it hadn’t. We looked into some of these cases and discovered

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 66 | Ross Anderson |

*2.5. THE SWAMP*

the No-PIN and preplay attacks on chip and PIN systems, which I’ll describe  
 in the chapter on banking (the bad guys had actually discovered these attacks,  
 but we replicated them and got justice for some of the victims).

Security researchers who discovered and reported vulnerabilities to a software

vendor or system operator used to risk legal threats, as companies sometimes  
 thought this would be cheaper than ﬁxing things. So some researchers took  
 to disclosing bugs anonymously on mailing lists; but this meant that the bad  
 guys could use them at once. By the early 2000s, the IT industry had evolved  
 practices of responsible disclosure whereby researchers disclose the bug to the  
 maintainer some months in advance of disclosure. Many ﬁrms operate bug-

bounty programs that offer rewards for vulnerabilities; as a result, independent  
 researchers can now make serious money selling vulnerabilities, and more than  
 one assiduous researcher has now earned over $1m doing this. Since the Stuxnet  
 worm, governments have raced to stockpile vulnerabilities, and we now see some  
 ﬁrms that buy vulnerabilities from researchers in order to weaponise them, and  
 sell them to cyber-arms suppliers. Once they’re used, they spread, are eventually  
 reverse-engineered and patched. I’ll discuss this ecosystem in more detail in the  
 chapters on economics and assurance.

Some more traditional sectors still haven’t adopted responsible disclosure.

Volkswagen sued researchers in the universities of Birmingham and Nijmegen  
 who reverse-engineered some online car theft tools and documented how poor  
 their remote key entry system was. The company lost, making fools of them-  
 selves and publicising the insecurity of their vehicles (I’ll discuss the technical  
 details in section 4.3.1 and the policy in section 27.5.7.2). Eventually, as soft-  
 ware permeates everything, software industry ways of working will become more  
 widespread too. In the meantime, we can expect turbulence. Firms that cover  
 up problems that harm their customers will have to reckon with the possibility  
 that either an internal whistleblower, or an external security researcher, will  
 ﬁgure out what’s going on, and when that happens there will often be an estab-  
 lished responsible disclosure process to invoke. This will impose costs on ﬁrms  
 that fail to align their business models with it.

**2.5** **The Swamp**

Our fourth category is abuse, by which we usually mean offences against the  
 person rather than against property. These range from cyber-bullying at schools  
 all the way to state-sponsored Facebook advertising campaigns that get people  
 to swamp legislators with death threats. I’ll deal ﬁrst with offences that scale,  
 including political harassment and child sex abuse material, and then with of-  
 fences that don’t, ranging from school bullying to intimate partner abuse.

**2.5.1** **Hacktivism and hate campaigns**

Propaganda and protest evolved as technology did. Ancient societies had to  
 make do with epic poetry; cities enabled people to communicate with hundreds  
 of others directly, by making speeches in the forum; and the invention of writing  
 enabled a further scale-up. The spread of printing in the sixteenth century led

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 67 | Ross Anderson |

*2.5. THE SWAMP*

to wars of religion in the seventeenth, daily newspapers in the eighteenth and  
 mass-market newspapers in the nineteenth. Activists learned to compete for  
 attention in the mass media, and honed their skills as radio and then TV came  
 along.

Activism in the Internet age started off with using online media to mobilise

people to do conventional lobbying, such as writing to legislators; organisations  
 such as Indymedia and Avaaz developed expertise at this during the 2000s.  
 In 2011, activists such as Wael Ghonim used social media to trigger the Arab  
 Spring, which we discuss in more detail in section 26.4.1. Since then, govern-  
 ments have started to crack down, and activism has spread into online hate  
 campaigns and radicalisation. Many hate campaigns are covertly funded by

governments or opposition parties, but by no means all: single-issue campaign  
 groups are also players. If you can motivate hundreds of people to send angry  
 emails or tweets, then a company or individual on the receiving end can have a  
 real problem. Denial-of-service attacks can interrupt operations while doxxing  
 can do real brand damage as well as causing distress to executives and staff.

Activists vary in their goals, in their organisational coherence and in the

extent to which they’ll break the law. There’s a whole spectrum, from the

completely law-abiding NGOs who get their supporters to email legislators to  
 the slightly edgy, who may manipulate news by getting bots to click on news  
 stories, to game the media analytics and make editors pay more attention to  
 their issue. Then there are whistleblowers who go to respectable newspapers,  
 political partisans who harass people behind the mild anonymity of Twitter  
 accounts, hackers who break into target ﬁrms and vandalise their websites or  
 even doxx them. The Climategate scandal, described in 2.2.5 above, may be  
 an example of doxing by a hacktivist. At the top end, there are the hard-core  
 types who end up in jail for terrorist offences.

During the 1990s, I happily used email and usenet to mobilise people against

surveillance bills going through the UK parliament, as I’ll describe later in sec-  
 tion 26.2.7. I found myself on the receiving end of hacktivism in 2003 when  
 the Animal Liberation Front targeted my university because of plans to build  
 a monkey house, for primates to be used in research. The online component  
 consisted of thousands of emails sent to staff members with distressing images  
 of monkeys with wires in their brains; this was an early example of ‘brigading’,  
 where hundreds of people gang up on one target online. We dealt with that  
 online attack easily enough by getting their email accounts closed down. But  
 they persisted with physical demonstrations and media harassment; our Vice-  
 Chancellor decided to cut her losses, and the monkey house went to Oxford  
 instead. Some of the leaders were later jailed for terrorism offences after they  
 assaulted staff at a local pharmaceutical testing company and placed bombs  
 under the cars of medical researchers [21].

Online shaming has become popular as a means of protest. It can be quite

spontaneous, with a ﬂash mob of vigilantes forming when an incident goes viral.  
 An early example happened in 2005 when a young lady in Seoul failed to clean up  
 after her dog defecated in a subway carriage. Another passenger photographed  
 the incident and put it online; within days the ‘dog poo girl’ had been hounded  
 into hiding, abandoning her university course [418]. There have been many

other cases since.

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 68 | Ross Anderson |

*2.5. THE SWAMP*

The power of platforms such as Twitter became evident in Gamergate, a

storm sparked by abusive comments about a female game developer made pub-  
 licly by a former boyfriend in August 2014, and cascading into a torrent of  
 misogynistic criticism of women in the gaming industry and of feminists who  
 had criticised the industry’s male-dominated culture. A number of people were  
 doxxed, SWATted, or hounded from their homes [1932]. The harassment was  
 coordinated on anonymous message boards such as 4Chan and the attackers  
 would gang up on a particular target – who then also got criticised by main-  
 stream conservative journalists [1130]. The movement appeared leaderless and  
 evolved constantly, with one continuing theme being a rant against ‘social jus-  
 tice warriors’. It appears to have contributed to the development of the alt-right  
 movement which inﬂuenced the 2016 election two years later.

A growing appreciation of the power of angry online mobs is leading politi-

cians to stir them up, at all levels from local politicians trying to undermine their  
 rivals to nation states trying to swing rival states’ elections. Angry mobs are an  
 unpleasant enough feature of modern politics in developed countries; in less de-  
 veloped countries things get even worse, with real lynchings in countries such as  
 India (where the ruling BJP party has been building a troll army since at least  
 2011 to harrass political opponents and civil-society critics [1637]). Companies  
 are targeted less frequently, but it does happen. Meanwhile the social-media  
 companies are under pressure to censor online content, and as it’s hard for an  
 AI program to tell the difference between a joke, abuse, a conspiracy theory and  
 information warfare by a foreign government, they end up having to hire more  
 and more moderators. I will return to the law and policy aspects of this in 26.4  
 below.

**2.5.2** **Child sex abuse material**

When the Internet came to governments’ attention in the 1990s and they won-  
 dered how to get a handle on it, the ﬁrst thing to be regulated was images of  
 child sex abuse (CSA), in the Budapest Convention in 2001. We have little data  
 on the real prevalence of CSA material as the legal restrictions make it hard  
 for anyone outside law enforcement to do any research. In many countries, the  
 approach to CSA material has less focus on actual harm reduction than it de-  
 serves. Indeed, many laws around online sexual offences are badly designed, and  
 seem to be driven more by exploiting outrage than by minimising the number  
 of victims and the harm they suffer. CSA may be a case study on how not to do  
 online regulation because of forensic failures, takedown failures, weaponisation  
 and the law-norm gap.

The most notorious forensic failure was Britain’s Operation Ore, which I

describe in more detail in 26.5.3. Brieﬂy, several thousand men were arrested  
 on suspicion of CSA offences after their credit card numbers were found on  
 an abuse website, and perhaps half of them turned out to be victims of credit  
 card fraud. Hundreds of innocent men had their lives ruined. Yet nothing was  
 done for the child victims in Brazil and Indonesia, and the authorities are still  
 nowhere near efficient at taking down websites that host CSA material. In most  
 countries, CSA takedown is a monopoly of either the police, or a regulated body  
 that operates under public-sector rules (NCMEC in the USA and the IWF in

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 69 | Ross Anderson |

*2.5. THE SWAMP*

the UK), and takes from days to weeks; things would go much more quickly if  
 governments were to use the private-sector contractors that banks use to deal  
 with phishing sites [938]. The public-sector monopoly stems from laws in many  
 countries that make the possession of CSA material a strict-liability offence.  
 This not only makes it hard to deal with such material using the usual abuse  
 channels, but also allows it to be weaponised: protesters can send it to targets  
 and then report them to the police. It also makes it difficult for parents and  
 teachers to deal sensibly with incidents that arise with teens using dating apps  
 or having remote relationships. The whole thing is a mess, caused by legislators  
 wanting to talk tough without understanding the technology. (CSA material is  
 now a signiﬁcant annoyance for some legislators’ staff, and also makes journalists  
 at some newspapers reluctant to make their email addresses public.)

There is an emerging law-norm gap with the growth in popularity of sexting

among teenagers. Like it or not, sending intimate photographs to partners

(real and intended) became normal behaviour for teens in many countries when  
 smartphones arrived in 2008. This was a mere seven years after the Budapest  
 convention, whose signatories may have failed to imagine that sexual images  
 of under-18s could be anything other than abuse. Thanks to the convention,  
 possessing an intimate photo of anyone under 18 can now result in a prison  
 sentence in any of the 63 countries that have ratiﬁed it. Teens laugh at lectures  
 from schoolteachers to not take or share such photos, but the end result is real  
 harm. Kids may be tricked or pressured into sharing photos of themselves,

and even if the initial sharing is consensual, the recipient can later use it for  
 blackmail or just pass it round for a laugh. Recipients – even if innocent – are  
 also committing criminal offences by simply having the photos on their phones,  
 so kids can set up other kids and denounce them. This leads to general issues  
 of bullying and more speciﬁc issues of intimate partner abuse.

**2.5.3** **School and workplace bullying**

Online harassment and bullying are a fact of life in modern societies, not just  
 in schools but in workplaces too, as people jostle for rank, mates and resources.  
 From the media stories of teens who kill themselves following online abuse,  
 you might think that cyber-bullying now accounts for most of the problem –  
 at least at school – but the ﬁgures show that it’s less than half. An annual  
 UK survey discloses that about a quarter of children and young people are  
 constantly bullied (13% verbal, 5% cyber and 3% physical) while about half  
 are bullied sometimes (24%, 8% and 9% respectively) [565]. The only national  
 survey of all ages of which I’m aware is the French national victimisation survey,  
 which since 2007 has collected data not just on physical crimes such as burglary  
 and online crimes such as fraud, but on harassment too [1458]. This is based on  
 face-to-face interviews with 16,000 households and the 2017 survey reported two  
 million cases of threatening behaviour, 7% were made on social networks and a  
 further 9% by phone. But have social media made this worse? Research suggests  
 that the effects of social media use on adolescent well-being are nuanced, small  
 at best, and contingent on analytic methods [1473].

Yet there is talk in the media of a rise in teen suicide which some commen-

tators link to social media use. Thankfully, the OECD mortality statistics show

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 70 | Ross Anderson |

*2.5. THE SWAMP*

that this is also untrue: suicides among 15–19 year olds have declined slightly  
 from about 8 to about 7 cases per 100,000 over the period 1990–2015 [1477].

**2.5.4** **Intimate relationship abuse**

Just as I ended the last section by discussing whistleblowers – the insider threat  
 to companies – I’ll end this section with intimate relationship abuse, the insider  
 threat to families and individuals. Gamergate may have been a ﬂashbulb exam-  
 ple, but protection from former intimate partners and other family members is  
 a real problem that exists at scale – with about half of all marriages ending in  
 divorce, and not all breakups being amicable. Intimate partner abuse has been  
 suffered by 27% of women and 11% of men. Stalking is not of course limited to  
 former partners. Celebrities in particular can be stalked by people they’ve never  
 met – with occasional tragic outcomes, as in the case of John Lennon. But for-  
 mer partners account for most of it, and law enforcement in most countries have  
 historically been reluctant to do anything effective about them. Technology has  
 made the victims’ plight worse.

One subproblem is the publication of non-consensual intimate imagery (NCII),

once called ‘revenge porn’ – until California Attorney General Kamala Harris  
 objected that this is cyber-exploitation and a crime. Her message got through  
 to the big service ﬁrms who since 2015 have been taking down such material on  
 demand from the victims [1690]. This followed an earlier report in 2012 where  
 Harris documented the increasing use of smartphones, online marketplaces and  
 social media in forcing vulnerable people into unregulated work including prosti-  
 tution – raising broader questions about how technology can be used to connect  
 with, and assist, crime victims [866].

The problems faced by a woman leaving an abusive and controlling husband

are among the hardest in the universe of information security. All the usual  
 advice is the wrong way round: your opponent knows not just your passwords  
 but has such deep contextual knowledge that he can answer all your password  
 recovery questions. There are typically three phases: a physical control phase  
 where the abuser has access to your device and may install malware, or even  
 destroy devices; a high-risk escape phase as you try to ﬁnd a new home, a  
 job and so on; and a life-apart phase when you might want to shield location,  
 email address and phone numbers to escape harassment, and may have lifelong  
 concerns. It takes seven escape attempts on average to get to life apart, and  
 disconnecting from online services can cause other abuse to escalate. After

escape, you may have to restrict childrens’ online activities and sever mutual  
 relationships; letting your child post anything can leak the school location and  
 lead to the abuser turning up. You may have to change career as it can be  
 impossible to work as a self-employed professional if you can no longer advertise.

To support such users, responsible designers should think hard about usabil-

ity during times of high stress and high risk; they should allow users to have  
 multiple accounts; they should design things so that someone reviewing your  
 history should not be able to tell you deleted anything; they should push two-  
 factor authentication, unusual activity notiﬁcations, and incognito mode. They  
 should also think about how a survivor can capture evidence for use in divorce  
 and custody cases and possibly in criminal prosecution, while minimising the

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 71 | Ross Anderson |

*2.6. SUMMARY*

trauma [1248]. But that’s not what we ﬁnd in real life. Many banks don’t really  
 want to know about disputes or ﬁnancial exploitation within families. A big  
 problem in some countries is stalkerware – apps designed to monitor partners,  
 ex-partners, children or employees. A report from Citizen Lab spells out the  
 poor information security practices of these apps, how they are marketed ex-  
 plicitly to abusive men, and how they break the law in Europe and Canada;  
 as for the USA and Australia, over half of abusers tracked women using stalk-  
 erware [1495]. And then there’s the Absher app, which enables men in Saudi  
 Arabia to control their women in ways unacceptable in developed countries; its  
 availability in app stores has led to protests against Apple and Google elsewhere  
 in the world, but as of 2020 it’s still there.

Intimate abuse is hard for designers and others to deal with as it’s entan-

gled with normal human caregiving between partners, between friends and col-  
 leagues, between parents and young children, and later between children and  
 elderly parents. Many relationships are largely beneﬁcent but with some abu-  
 sive aspects, and participants often don’t agree on which aspects. The best

analysis I know, by Karen Levy and Bruce Schneier, discusses the combination  
 of multiple motivations, copresence which leads to technical vulnerabilities, and  
 power dynamics leading to relational vulnerabilities [1154]. Technology facil-  
 itates multiple privacy invasions in relationships, ranging from the casual to  
 serious abuse; designers need to be aware that households are not units, devices  
 are not personal, and the purchaser of a device is not the only user. I expect  
 that concerns about intimate abuse will expand in the next few years to con-  
 cerns about victims of abuse by friends, teachers and parents, and will be made  
 ever more complex by new forms of home and school automation.

**2.6** **Summary**

The systems you build or operate can be attacked by a wide range of oppo-  
 nents. It’s important to work out who might attack you and how, and it’s also  
 important to be able to ﬁgure out how you were attacked and by whom. Your  
 systems can also be used to attack others, and if you don’t think about this in  
 advance you may ﬁnd yourself in serious legal or political trouble.

In this chapter I’ve grouped adversaries under four themes: the spooks, the

crooks, the hackers and the swamp. Not all threat actors are bad: many hack-  
 ers report bugs responsibly and many whistleblowers are public-spirited. (‘Our’  
 spooks are of course considered good while ‘theirs’ are bad; moral valence de-  
 pends on the public and private interests in play.) Intelligence and law enforce-  
 ment agencies may use a mix of traffic data analysis and content sampling when  
 hunting, and targeted collection for gathering; collection methods range from  
 legal coercion via malware to deception. Both spooks and crooks use malware  
 to establish botnets as infrastructure. Crooks typically use opportunistic col-  
 lection for mass attacks, while for targeted work, spear-phishing is the weapon  
 of choice; intelligence agencies may have fancier tools but use the same basic  
 methods. There are also cybercrime ecosystems attached to speciﬁc business  
 sectors; basically, crime will evolve where it can scale. As for the swamp, the  
 weapon of choice is the angry mob, wielded nowadays by states, activist groups

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 72 | Ross Anderson |

*2.7. RESEARCH PROBLEMS*

and even individual orators. There are many ways in which abuse can scale,  
 and when designing a system you need to work out how crimes against it, or  
 abuse using it, might scale. It’s not enough to think about usability; you need  
 to think about abusability too.

Personal abuse matters too. Every police officer knows that the person who

assaults you or murders you isn’t usually a stranger, but someone you know  
 – maybe another boy in your school class, or your stepfather. This has been  
 ignored by the security research community, perhaps because we’re mostly clever  
 white or Asian boys from stable families in good neighbourhoods.

If you’re defending a company of any size, you’ll see enough machines on your

network getting infected, and you need to know whether they’re just zombies on  
 a botnet or part of a targeted attack. So it’s not enough to rely on patching and  
 antivirus. You need to watch your network and keep good enough logs that when  
 an infected machine is spotted you can tell whether it’s a kid building a botnet  
 or a targeted attacker who responds to loss of a viewpoint with a scramble to  
 develop another one. You need to make plans to respond to incidents, so you  
 know who to call for forensics – and so your CEO isn’t left gasping like a landed  
 ﬁsh in front of the TV cameras. You need to think systematically about your  
 essential controls: backup to recover from ransomware, payment procedures to  
 block business email compromise, and so on. If you’re advising a large company  
 they should have much of this already, and if it’s a small company you need to  
 help them ﬁgure out how to do enough of it.

The rest of this book will ﬁll in the details.

**2.7** **Research problems**

Until recently, research on cybercrime wasn’t really scientiﬁc. Someone would  
 get some data – often under NDA from an anti-virus company – work out some  
 statistics, write up their thesis, and then go get a job. The data were never  
 available to anyone else who wanted to check their results or try a new type of  
 analysis. Since 2015 we’ve been trying to ﬁx that by setting up the Cambridge  
 Cybercrime Centre, where we collect masses of data on spam, phish, botnets  
 and malware as a shared resource for researchers. We’re delighted for other  
 academics to use it. If you want to do research on cybercrime, call us.

We also need something similar for espionage and cyber warfare. People

trying to implant malware into control systems and other operational technology  
 are quite likely to be either state actors, or cyber-arms vendors who sell to  
 states. The criticisms made by President Eisenhower of the ‘military-industrial  
 complex’ apply here in spades. Yet not one of the legacy think-tanks seems  
 interested in tracking what’s going on. As a result, nations are more likely to  
 make strategic miscalculations, which could lead not just to cyber-conﬂict but  
 the real kinetic variety, too.

As for research into cyber abuse, there is now some research, but the tech-

nologists, the psychologists, the criminologists and the political scientists aren’t  
 talking to each other enough. There are many issues, from the welfare and rights  
 of children and young people to our ability to hold fair and free elections. We

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 73 | Ross Anderson |

*2.8. FURTHER READING*

need to engage more technologists with public-policy issues and educate more  
 policy people about the realities of technology. We also need to get more women  
 involved, and people from poor communities in both developed and less devel-  
 oped countries, so we have a less narrow perspective on what the real problems  
 are.

**2.8** **Further Reading**

There’s an enormous literature on the topics discussed in this chapter but it’s  
 rather fragmented. A starting point for the Snowden revelations might be Glen  
 Greenwald’s book *‘No Place to Hide’* [816]; for an account of Russian strat-  
 egy and tactics, see the 2018 report to the US Senate’s Committee on Foreign  
 Relations [385]; and for a great introduction to the history of propaganda see  
 Tim Wu’s *‘The Attention Merchants’* [2050]. For surveys of cybercrime, see our  
 2012 paper “Measuring the Cost of Cybercrime” [90] and our 2019 follow-up  
 “Measuring the Changing Cost of Cybercrime” [91]. Criminologists such as Bill  
 Chambliss have studied state-organised crime, from piracy and slavery in pre-  
 vious centuries through the more recent smuggling of drugs and weapons by  
 intelligence agencies to torture and assassination; this gives the broader context  
 within which to assess unlawful surveillance. The story of Gamergate is told in  
 Zo¨e Quinn’s *‘Crash Override’* [1567]. Finally, the tale of Marcus Hutchings, the  
 malware expert who stopped Wannacry, is at [811].

|  |  |  |
| --- | --- | --- |
| **Security Engineering** | 74 | Ross Anderson |