Extract from Digital Dangers

Janice Acquah

This is an extract from the programme *Digital Dangers* recorded for the Open University course T305 *Digital Communications*. You will hear about UK government strategies for combating attacks on communication systems, particularly in response to the terrorist attacks in the USA on 11th September 2001. Representatives of government agencies discuss the actions being taken, potential threats and the implications of new legislation for all Internet users.

[Archive from BBC/OU programme 'Hack the Planet']

Alexei Sayle (Presenter –'Hack the Planet')

No computer-related activity generates more fear and misunderstanding than computer hacking.

Hacker (anonymity preserved)

We will find a way in, and sometimes it can take just a matter of minutes.

Alexei Sayle

Teenagers take over computers, just for the thrill. White-collar criminals enjoy using computers for fraud or espionage.

Keith Dawson (Net journalist)

Operating systems that run the Internet are not secure.

Alexei Sayle

Everyone who uses the Internet is at risk.

[End of archive material]

Winifred Robinson (Presenter)

One of the issues behind all this, is how we view the communication infrastructure. Is it a commodity you buy and you get what you pay for, or is it more important than that? But the way we view our connected world has changed since the terrorist attacks. Andrew Pinder is the UK government e-envoy, and part of his remit is to ensure the reliability of CNI, the critical national infrastructure of the UK. So what exactly is CNI?

Andrew Pinder

Well the critical national infrastructure are those things that exist in this country, on which our economy, or our way of living depends. So what would we regard those as? Well, often, quite a big chunk of government. If you had, for example, the benefit systems going down completely, then after a while, that would hurt people who particularly need a benefit. If you've got utility systems like the power supplies or water going down, that was clearly part of the critical national infrastructure, and they need protecting. So, there are those sorts of installations

and networks of things, which would need to be protected, both physically, and electronically. And one of the things we'd want to make sure is that someone like a power company or a utility company aren't vulnerable to, in my case, an electronic attack, a hacker trying to get in and bring them down. And so we pay particular attention to making sure that they're kept in touch with the latest threats, and advise on how to counter the latest threats. And our track record on that, events proved, has been pretty good.

Winifred Robinson (Presenter)

But your answer implies that national utilities companies are connected to the web.

Andrew Pinder

Well in some respects they are of course. But they're also connected to their own networks, and the national grid, for example, clearly has to be highly dependent upon IT. And therefore, we're not just protecting those sorts of installations against external attack across the web, where you can put in place either physical separation or very strong firewalls, but you're also wanting to guard against internal interference, someone inside introducing a virus. You want to make sure they do sensible things here. So, looking at our own systems here, we try to make sure that we're reasonably well protected both from internal attack – and we do things like vet our employees, but also make sure our systems are robust – but also from external attacks – we've got firewalls in place. And that's what grown-up companies do, and we just want to make sure that those companies, which are particularly crucial to the national infrastructure, do it particularly well, and they do.

Winifred Robinson (Presenter)

The Communications Electronic Security Group, CESG for short, is part of GCHQ, and it works with the UK government, to ensure the country's national infrastructure is secure. You might not have heard of them before, but they've been around for some time. Richard Walton, director of CESG, explains.

Richard Walton

CESG is the national technical authority for information assurance, and our roots go back, really to the end of the Second World War, when our major concern was that our own government's military and diplomatic communications were protected, by ciphers, in such a way that other countries couldn't have the success that we had had during the War against Enigma, which of course is now well known. Since then, as you know, the world has moved a long way in this area, and we have evolved with that. So, whereas our original strengths were in ciphers, and in communications security, we have now developed the skills in protection of more general information systems, particularly computers and networks of computers.

Winifred Robinson (Presenter)

Does Richard Walton believe our national infrastructure's dependent on sectors identified by Andrew Pinder, on digital communication networks such as the Internet?

Richard Walton

I think all are dependent to some extent, and getting more dependent, and I think that's really the crucial thing. I mean, government itself, under the modernising government initiative, has been busy wiring itself up, wiring up its services in a way that they're becoming increasingly dependent.

Winifred Robinson (Presenter)

When we talk about the vulnerabilities that rise from these systems, are they viruses, hackers? Richard Walton again.

Richard Walton

In some sense I'm concerned about the lot. There are the hackers, the very visible, rather amateur people. These people should not be glorified in a technical way. They're not smart. There's more surgical attack, which would be designed not to be noticed, and is of far more concern to us, and how we actually stop, or detect things that are going on, perhaps in readiness for a hostile situation. Remember that the first thing that we did on the outbreak of the Second World War, was we cut the transatlantic cables, that the Germans could use, and denying service to your information systems is not a new threat. It is one of the first things that an enemy would seek to do in warfare, to deny the command and control of their potential enemy. And, the thing that we still feel could bring a western economy to its knees, would be appropriate disruption of the – again it's really the command and control systems. They happen now to be computer networks, or computer network driven, in almost all cases.

Winifred Robinson (Presenter)

But we are vulnerable to viruses, and one particular virus caused chaos in many systems. It was the love bug. Richard Walton explains.

Richard Walton

The major feature of the love bug that caused damage was the speed with which it spread. The actual technology that was used was pretty unsophisticated. The programming was appalling, so it wasn't actually very clever, it wasn't very well executed, yet it did an enormous amount of damage, not so much of itself – it wasn't carrying a payload as such – but through overloading the networks, by its means of propagation, which is essentially to send itself to everybody in your address book. And that just clogged up the wires in traditional terms, and brought servers down, and brought systems down, thereby causing damage, and doing it so quickly that there was difficulty in reacting.

Winifred Robinson (Presenter)

So what would be a real cause for concern?

Richard Walton

Now what one really fears is malicious software that hides itself better, that is not, does not make itself, apparent, that strikes when the strike will do most damage. Now of course if it is a strike that hits availability in a serious way, people in a sense will know they've been had. It is perfectly possible to hide even the effects of a disruptive program, for a while, and to separate it in time from its original promulgation, to make it not have as much of a signature as so many of these do. And that is just that much more insidious, that much more difficult. You

spread it before the damage is apparent, that's what I really fear, and you then may be able to do selective damage, of a much more serious nature.

Winifred Robinson (Presenter)

Since the terrorist attacks in New York and Washington, Andrew Pinder can't afford to be complacent. What are they doing to prevent terrorists attacking the country's infrastructures?

Andrew Pinder

We can't have a sort of twin tower sort of problem, with the Internet infrastructure in this country and, that's partly my job, and you know I picked up that role alongside some other roles per September 11th. So, we do that, you know, we talk to the Internet service providers and the providers of the infrastructure, to understand what the risks are, and talk to them about the risks, and make sure that they understand them, and make sure that we've got a robust Internet environment, and a telecoms environment, that can withstand the sorts of disasters that happened in New York and Washington. And I think we're in decent shape. I think if a Boeing 747 landed on a particular site, then there will be clearly local problems, but it would affect the whole country? No it wouldn't. We've done some good things there, and worked very hard at that.

Winifred Robinson (Presenter)

Casper Bowden is the director of FIPR, the Foundation for Internet Policy Research. Bowden has opposed anti-terrorist legislation, since it was hurried through by the UK government after the events of September 11th. But why does he oppose it?

Casper Bowden

Part 11 of the Anti-Terrorism Crime and Security Act deals with powers which can compel Internet providers, and in fact, potentially any Internet user, to stockpile traffic data, on their computer. What this means in practice, is that information recording the whereabouts of your mobile phone for example, potentially to a few metres resolution, the websites that you read, and who you're in contact with on the Internet, will now be recorded by your Internet provider, for between a few days and up to a year, depending on the nature of the information, and this will be done for everyone in the country. The Anti-Terrorism Act interacts with two other Acts of Parliament, the Data Protection Act and the Regulation of Investigatory Powers Act 2000. RIP creates the powers to get at the data, once it's been collected, and the Anti-Terrorism Act has now created the power to insist that the data is collected. The Data Protection Act governs what limits there are, if any, on how that data could be processed automatically. Using very powerful software on supercomputers, linkages, and unknown patterns, can be discovered in huge amounts of data in a process called data mining. In this case, information contained in traffic data really reveals a pretty complete map of somebody's private life, even though there is no access to the content of the communications. The pattern is sufficient to lay out in very great detail what is going on in somebody's inner life.

Winifred Robinson (Presenter)

So what is traffic data, and what's meant then by traffic analysis? Casper Bowden.

Casper Bowden

Traffic data is signalling or controlling information in a communications system. So it isn't the essential content of the message, it's the addressing information which lets the message get from A to B. In the case of a telephone system, this is simply a list of numbers incoming, or calls outgoing, but the Internet works in many different ways from the telephone system. So, for example, if I know the address of a page on the worldwide web, then I know what you've read on the worldwide web in most cases. Similarly, if I know the address of the web page that you submit to a search engine, I know what you've been searching for, what your interests are. So, the way in which the Internet is used creates a much more complete and intrusive map of somebody's private thoughts and intentions than does the usage of the telephone system. Civil libertarians, or cyber libertarians, are arguing that the power that computers have to analyse this traffic data automatically, mean that it is not comparable to the historical situation of accessing paper records, and that in fact, this creates an entirely new form of mass surveillance.

Winifred Robinson (Presenter)

Whereas Casper Bowden and others believe that this traffic data is infringing on our civil liberties, Andrew Pinder has other thoughts.

Andrew Pinder

Well I think in the area of the Regulatory and Investigatory Powers Act, which was passed last year, there are two sorts of issues that people get worried about. One is the privacy issue. Is this too great an interference in our privacy and our personal lives? Are we subject to unrestrained hacking by law enforcement agencies? And the answer to that is no. I mean the Act puts in place the same sorts of safeguards and constraints that would apply to, for example, telephone interception. So, people have got to get a court order and an order from a senior minister to authorise, for a limited period at a time, an intercept. The same sorts of principles are applied to the question of whether we can try and look at somebody's e-mails or not. So it's quite a big deal, and it's not something that's done routinely, but at the same time, got to balance the worries about privacy against the worries about personal safety and national security, and criminal activity, pornography and so on. And therefore, the right thing to do is to have the powers, but then have constraints around the powers, and rules around the powers to make sure the powers are properly used. That's what we're trying to do in that area.

Winifred Robinson (Presenter)

But what significance does September 11th have in all of this? Casper Bowden again.

Casper Bowden

If we look at the modus operandi of the 11th September terrorists, it appears from public reports that they used web-based e-mail services, from public terminals in libraries or cafes, and this is a much better way of communicating covertly than the use of encryption. Encryption is still relatively rare on the net, and it is also very easy to detect, because it has a peculiar signature, in terms of its density of information. Therefore, you would have to be a particularly daft kind of terrorist to use that for your covert communications, as opposed to using

veiled language – just a pre-agreed meaning attached to an otherwise innocuous phrase – and that of course is something which can never be detected by some kind of automatic scanning system. So, the omniscience that the intelligence agencies appear to want over Internet communications, I think is illusory, it's simply unachievable.

Winifred Robinson (Presenter)

The new Act will mean millions of bytes of information sent through the Internet will be stored, but how?

Casper Bowden

The black boxes themselves really don't do anything more than what a technician would call a packet sniffer. It simply looks at every packet of information flowing along the network, and makes a copy of it, or arranges for it to be forwarded. There is an outstanding issue, to do with different types of warrant in the RIP Act. There are actually two types. The first is a targeted warrant, the other is what can only be described as a trawling warrant. It's a general entitlement to search through vast volumes of communications, looking for particular concepts or keywords. It's possible that the black boxes will have to be engineered to cope with executing one of the trawling warrants. In other words the Internet provider would effectively become a sub-branch of GCHQ, and it would then begin trawling through the entire flow of data, of all its customers, in a sort of massive distributed search.

Janice Acquah

This is the end of the audio extract.

DIRECTOR: Ian Black
PA: Helen Lowery

MAIN CONTRIBUTORS:
Winifred Robinson Presenter
Andrew Pinder Interviewee – Government E-envoy spokesman
Richard Walton Interviewee – Director of CESG, Internet security expert
Casper Bowden Interviewee – Director of FIPR (Foundation for Information Policy Research)