Print This Article

<< Return to Funding the new Home Guard to protect against cyber attacks

Funding the new Home Guard to protect against cyber attacks

Derek Parkinson
January 03 2011

For the first time, cyber threats are on the fast track to the Prime Minister's in-tray. And with £650 million available, the Government is putting its money where its mouth is, says **Derek Parkinson**.

Much of the Strategic Defence and Security Review (SDSR) of October 2010 had a familiar ring to it. It contained a commitment to a more 'joined-up' approach within government, recognition that closer working with industry is essential to protecting our economic wellbeing and our critical national infrastructure and acknowledged that citizens need better information about cyber crime and the sources of help available to tackle it.

Similar commitments were made by the previous Labour administration as part of its Cyber Security Strategy of June 2009, which fleshed out ideas contained in the Digital Britain report of the same year.

So, what is new and noteworthy? Given the cuts in public spending, it was perhaps no surprise that the £650 million of extra funding over the next four years has grabbed a lot of the attention. Obviously, it is a significant commitment in a time of austerity, but there are other important developments to note.

The SDSR builds on the National Security Strategy, a broad-brush assessment of the threats the UK faces and the coalition government's approach to tackling them. For the first time, cyber threats are on the fast track to the Prime Minister's in-tray, alongside terrorism, natural disasters and military actions by hostile states. Cyber security is now an issue of political leadership for the PM, not just something for technocrats and civil servants to worry about.

The details of exactly how the £650 million is to be parcelled out as part of the new National Cyber Security Programme will be decided behind closed doors in Whitehall over the coming months. What we do know is that the funds will have to spread widely over numerous government departments and bodies and that a coordinating role will be played by the Office of Cyber Security from within the Cabinet Office. There are five major strands to the new programme:

- The UK Defence Cyber Operations Group, set up in October, will work with the Ministry of Defence to add cyber warfare capabilities to our armed forces
- The main UK intelligence agencies – GCHQ, MI6 and MI5 – will develop their capability to gather intelligence about cyber security and share it
- A cyber infrastructure team in the Department for Business, Innovation and Skills (BIS) will be responsible for engaging with key UK industries
- More money for existing initiatives, such as Get Safe Online for citizens, while the Home Office develops a cyber crime strategy that includes a single point of contact for citizens and businesses

- A new Infrastructure Security and Resilience Advisory Council will encourage closer working with private sector national infrastructure providers, such as the water, telecommunications and civil nuclear industries.

Infinite variety

The threats that the SDSR is designed to counter are extremely varied. In part, this reflects broad changes across our society – most obviously, how much we depend on technology in our personal lives, our work and for access to essential services.

For these reasons, we are exposed to risk, whether it be from failures and accidents, or attacks from criminals, terrorists or nation states. The SDSR makes the reasonable assumption that our dependence on technology and the deliberate attacks on it are set to increase.

Crime is a key concern. Between 2008 and 2009, there was a 14 per cent increase in online banking losses due to fraud, while 51 per cent of all the malicious software threats that have ever been identified came to light in 2009.

Moreover, it is likely that official figures seriously underestimate the true scale of the problem. “Police forces are not even geared up to prosecute ‘small' online crimes,” says professor Denis Edgar-Nevill, chair of the cyber crime forensics group at the British Computer Society. “Then there is the question of how many crimes actually get reported. We tolerate it as the price for having the freedom the internet gives us. The threshold where things get bad enough for people to report a crime is going up and up.”

Breaches of security cost businesses dearly too. A recent report from the Parliamentary IT Committee (Pitcom) noted that in 2008 the worst IT security incident cost businesses between £10,000 and £20,000 on average. The cost rises with the size of the company – for large businesses, it can be anywhere between £90,000 and £170,000; for very large ones, it can reach £1 million or £2 million.

The threats are growing not only in number, but in sophistication also. A clear example of this is the emergence of the Stuxnet malware, apparently designed to exploit vulnerabilities in Windows OS and commercial software used to control processes in large industrial plants, such as factories or power stations (including, worryingly, nuclear). This complexity, coupled with estimates that the bulk of infections appeared to be located in Iran, have given rise to a great deal of speculation that Stuxnet was developed as part of some cyber warfare programme by actors as yet unknown.

Many experts are cautious when asked what we can definitely infer from the technical details of Stuxnet. “What its ultimate purpose is I wouldn't be able to say – partly because I haven't reverse-engineered it,” says Ross Anderson, professor of security engineering at Cambridge University Computer Laboratory. “What we can say is that it was probably written by five people in about six months – we know this because of the time stamps all over it. It was almost certainly written by people who write malware as a living. The original claims about zero-day vulnerabilities turn out to be overestimates,” he says.

National Infrastructure vulnerabilities

Analysing threats to civilian life in the UK has been the business of government since long before cyber threats. Much of this work – coordinated by the Cabinet Office's Civil Contingencies Secretariat (CCS) – has focused on vulnerabilities within our National Infrastructure (NI).

The NI delivers the services that are essential to the safety and stability of the UK population – energy, transport, water, food, financial services and information and communication technologies (ICTs). Threats to NI typically include short-term events such as natural disasters, or longer-term trends, whether they be demographic shifts, changes in the climate or depletion of natural resources.

It has long been recognised that parts of our NI are interdependent – and that energy supply is the most crucial. It has always been a concern that there is a risk of a domino effect, with failures in one part of NI triggering failures in another. In the worst case, this process runs out of control, leading to catastrophe.

More recently, there has been growing awareness that our rapidly acquired dependence on ICTs brings with it new risks, along with all the benefits. It makes keeping pace with the risks and working out how to contain them a much greater challenge. Not so long ago, the internet didn't even exist, but now, if your granny needs internet access for her food shopping as part of living an independent life, then it's an essential service, as Civil Contingencies Secretariat chief Bruce Mann once pointed out.

Beyond this kind of dependence, ICTs have had a more subtle and pervasive effect, making the interconnections and dependencies between parts of our NI more complex than ever before. In simple terms, it is less easy to see what will cause all the dominos to come crashing down.

Among others, the Council for Science and Technology (CST) and the Royal United Services Institute (RUSI) have warned that it should be an urgent priority to improve our understanding of how vulnerable our NI is to cyber attack.

At least 80 per cent of our NI is owned by the private sector. It is overseen by a patchwork of regulatory bodies – and in some cases, not at all. In other cases, the regulatory framework has been in place for more than 20 years and was designed for a simpler, less connected world, not the challenges of the 21st century.

According to the CST, the highly interconnected nature of our NI, coupled with the fragmentation of delivery and regulatory oversight, means that:

- No one is responsible for looking across the NI as a whole
- There is little or no knowledge of vulnerabilities and risk arising from interdependencies across the NI
- Little or no expenditure occurs on a precautionary basis; instead, the approach is to perform heroic acts in times of crisis.

The fragmented ownership and regulatory control is replicated at the level of our ICT infrastructure and this is one of the most challenging difficulties we face, says RUSI.

Could a cyber attack really knock out part or even all of our NI? “It's difficult to judge what the true threat is. We're seeing some indications and we're hearing some horror stories. I wouldn't see it in terms of the apocalypse, it is more likely to be the discovery of vulnerability from time to time,” says Edgar-Nevill.

But even threats that aren't obviously apocalyptic may still be serious, deserving urgent attention, suggests Pitcom chairman, Alun Michael MP. “Arguably, the challenge of security on the internet is the most complex issue we have ever faced. And the challenges range through sophisticated attacks by crooks who treat the internet like a market, to the security of individual data and the spam/phishing attacks that cause widespread irritation.

“At least we can just ignore the bottom end of all that, can't we? Well, no, that's a mistake,” said Michael. “Those who know most about the operation of serious crooks and terrorists are the quickest to understand the connection between a lot of ‘stuff' that just looks like the sort of interference that blighted the earliest cat's whisker radios and the serious threats to society.

“Serious crime gets the headlines, but the things that undermine people's confidence in the security of their local neighbourhood are graffiti and incivility. Given that public confidence is important, it's a mistake to think you can just ‘concentrate on the serious stuff',” said the MP.

Murky prospect – cyber warfare

There has been a lot of speculation about whether we have already seen intentional acts of cyber warfare and, if so, who was behind them. What we can say with certainty is that we have witnessed attacks on the kind of scale – and with the sort of target – that would be expected of cyber warfare.

The 2008 attacks against Georgian infrastructure and government websites that accompanied fighting between Georgian and Russian troops and the massive denial-of-service attacks against government and private sector websites in Estonia in April and May 2007 are clear examples.

These developments raise difficult questions. What actions constitute acts of war in cyberspace? How do these fit within our framework of military ethics? Is international law able to deal with them?

“It is important to distinguish cyber espionage, cyber attacks in general and true cyber warfare,” says philosophy professor Randy Dipert of the State University of New York at Buffalo, who was formerly a military ethicist at West Point.

“There seems to be a widespread understanding, without a stated treaty or explicit policy, that no amount or kind of espionage is sufficient, by itself, to trigger a morally justified war,” he says.

“What is new is cyber attacks by organised groups of hackers acting under the command of some government. We know some nations have such groups, located under military control and organised for attacking other governments and national industries – China, North Korea, Israel, Iran and the US have publicly said they have such efforts and there are probably many more, such as Russia,” Dipert says.

“If cyber attacks result in deaths or permanent destruction, they are covered by international law. Killing military or civilian individuals is an act of war – even as an unintended side-effect – but in war, civilian lives may be lost and civilian objects – water systems etc – destroyed only in the pursuit of a legitimate military objective.”

We have yet to see policies for containing these threats – what roles deterrence, or purely defensive measures, or international treaties will play, says Dipert. “I have challenged officials in the Defense Department about this and it was clear it was too hot for them to say anything, even speculatively.”

A key difficulty in responding to cyber attacks is attribution – identifying who is behind them, says professor Peter Sommer of the information systems integrity group at the London School of Economics. “The attacking computers may be ‘innocent'. A lot of ideas that are part of traditional thinking about defence then don't work – such as deterrence, for example,” he adds.

“What we have seen so far may well have been the flexing of muscles,” says Sommer. And although the UK's cyber defences are constantly probed, this may be to test their vulnerabilities rather than to prepare for an all-out attack, he suggests.

True cyber warfare is unlikely to be pursued in isolation from conventional military operations, says Sommer. “It will be used in initial skirmishes, to cause confusion. We'll see that more and more, but the pure cyber war isn't a goer, in my view.”

Government can't do it all

How far can we depend on the UK Government to protect us from cyber threats? In the case of cyber warfare, we have little choice but to rely on its wisdom in international relations, alliances and conventional military capabilities. Can we assume an offensive cyber capability will be developed too?

“It's not the sort of thing that gets talked about openly, but I think work is going on in that area,” says Andy Hull, senior research fellow at think-tank, the Institute for Public Policy Research. “I remember talking to a senior government scientist off the record and being told that the kind of Mutually Assured Destruction (‘MAD') we faced in the Cold War is not beyond the bounds of credibility.”

It may be difficult to resist developing an offensive capability, but it is only part of the picture, suggests LSE visiting professor, Peter Sommer. “When you look at conventional weaponry, to have an offensive capability you need planes, ships and tanks. With cyber you can argue you don't need new hardware.”

An offensive cyber capability may have limitations. “It may turn out to be similar to biological weapons – can you gauge the effects, how do you know they won't bite you back? I think our main defence will be resilience, plus contingency planning,” he says.

What if resilience fails? Experts have serious doubts about how able the Government is to respond to a fast-moving crisis. The main worry is that there is no single department or agency empowered to take control of a crisis.

The role of the Cabinet Office Civil Contingencies Secretariat is to ‘hold the fort' until a lead department takes over – in the case of a major road incident, for example, it would be the Department for Transport. The potential difficulty with this is posed by the sort of fast-moving crisis that crosses departmental lines of responsibility, ie just the kind of threat that a major cyber security incident poses.

“The Government is locked into silos and it knows the limitations of this,” says Peter Power, managing director of Visor Consultants, a specialist in crisis management. “But if you had a single body in central government, you would need a minister – and who wants to be minister for disasters?”

If we can't have a minister for disasters, do we perhaps need a minister for cyber security? Labour MP Alun Michael is unconvinced. “It's a myth to think that more gets done just because you have one person exercising leadership. That myth led to governments appointing ‘tsars' to ‘take a grip' on policy areas from drugs to farming. Generally, it didn't work. Why not? It can only work if there is a simple solution and all that is needed is for heads to be banged together. So the first fact is that Government alone can't deliver security to the internet. And the second fact is that no one minister and no one department can do it all,” he says.

Most observers view recent Government moves as a positive development. “One way of seeing this £650 million is, finally, as a validation of CISOs,” says Henry Harrison, technical director at consultancy Detica. “And it's not all about threats. Iain Lobban [director of GCHQ] recently talked about the opportunities of a global market – a unique example of Government being ahead of industry in recognising commercial opportunities, because it has access to the intelligence,” he says.