WEAPONISING THE INTERNET

Michael Clarke *examines cyber terror attacks and asks if they are certainly virtual or virtually certain?*

"Cyber terrorism is the dog that didn't bark' said former MI5 chief Lord Evans of Weardale at the launch of the Countering Jihadist Terrorism in the UK initiative. It wasn't clear, he said, why this might be so, given the natural vulnerability of modern societies to cyber attack; and we should be ready to deal with it as and when it might start to happen. Certainly, he said, the full spectrum of likely terror threats and responses should be part of the national conversation that CoJiT-UK is designed to start. So why hasn't that dog barked and what will happen when it does?

It isn't as if terrorist groups ignore the power of cyber space to further their campaigns. Indeed, almost all terrorist groups, and certainly the proselytising ones like the jihadists, see it as a vital weapon in their armoury. But cyber power in the service of a terrorist group is not the same as cyber terrorism in the sense that the former MI5 chief warned about.

Sophisticated cyber power offers terrorist groups the prospect of using the internet both as a vast underground network – of unknown and growing size – where they can hide their information, material and identities; as well as a burgeoning city on the surface where they can hide in plain sight while they extort money, create their own version of reality, threaten and cajole the vulnerable. The potential to operate simultaneously (and cheaply) both underground and over ground has changed the established nature of 19th and 20th-century terrorism forever.

As a domain of criminality (and hence of policing) the world wide web has no spatial or temporal limits. No one knows how big the internet currently is. Only indices of its likely size can be estimated. CISCO has estimated that by 2019 annual internet traffic will have reached 2 zettabytes, while Gartner Inc estimates that over 4 zettabytes of content is already stored across the internet. Certainly, no one knows the extent of the dark web. And in terms of criminality and terrorism the open web offers the key advantages of communication platforms and an array of apps. Even the most obvious names suggest orders of magnitude more than precise numbers. Facebook has over two billion users, WhatsApp around 500 million, Instagram around 600,000 and Twitter over 330 million. Facebook estimates that, on average, written material or images are distributed by one of its users (liked or shared) almost 10 million times a day. In March 2017 the five internet market leaders were responsible for supplying more than 6.5 million different apps, the majority capable of being misused, one way or another, for terrorist purposes. Apple estimates that by September 2016 its 2.2 million apps had been cumulatively downloaded around 140 billion times.

EVOLVING LANDSCAPE

So as long as they remain nimble across the ground-level city of the open net and the underground vastness of the dark web, terror groups can use their cyber power to reinforce messages among the committed, inspire new followers, distribute information and skills and to do a great deal of specific attack planning. The old terrorist model of cell structures – where a small cell of three or four people had only a thin and tenuous contact with any other cell in the organisation – has been turned on its head. Now, terror groups openly connect themselves; franchise their operations and issue broad campaign calls. From 2012 Islamic State's Mohammad al-Adnani regularly called on jihadists everywhere to use rocks, knives, cars, poisons, choking and any methods they could find to kill Westerners – a call that seems to have inspired Michael Adebolajo and Michael Adebowale to murder Gunner Lee Rigby in the street in 2013. Anis Amri drove a lorry into shoppers in Berlin's Christmas market in 2016 and three similar attacks followed in and around London in 2017, alongside two homemade bomb attacks in Manchester and London with devices and planning directed from the dark web. Modern terrorists have effectively weaponised the communications of the web in ways that could scarcely have been anticipated even 20 years ago.

So why hasn't the web itself been directly weaponised? Where are the 'cyber bombs', the 'city stoppers', the 'cyber poisons'? They may be coming. That was Lord Evans' point. And the advent of more sophisticated 3D printing technologies – 'additive manufacturing' – suggests some truly worrying possibilities. Allied with innovations in materials science, the possibilities of amateurs being able to get hold of basic materials of sufficient quality and then remotely access a manufacturing process they need know nothing about to create firearms and explosive or chemical devices would constitute a new dimension in networked terror. With so much technology operating in their favour, why don't the terrorists launch outright cyber wars against us?

Many writers have worried that 'cyber wars' could replace more traditional sorts of combat, where cyber attack makes living intolerable to the point where a society capitulates to the pressure – human misery without violent destruction. But most analysts realise how difficult this would actually be to achieve. Modern societies are more akin to rapidly flowing water than to pieces of machinery or architectural constructs. They can certainly be inconvenienced or disrupted, but in truth it's harder to incapacitate them than most thriller writers like to assume.

THERE IS NO OBVIOUS TECHNOLOGICAL PLATEAU TO LIMIT HOW DISRUPTIVE CYBER ATTACKS COULD BE

Nevertheless, Western security planners are increasingly concerned at how vulnerable their own critical national infrastructures (CNIs) have become with the intrinsic digitisation of all industrial control systems. Public utilities, transport, communication links, health provision and Government data in most countries are protected by obsolete cyber security. They become networked in ways their own original designers no longer understand. Cyber attackers are known to have broken into sensitive military installations in other countries by penetrating systems operating subsidiary services, such as the street lighting outside them. The fact that Britain's CNI is vulnerable is well understood by security chiefs, but the depth and extent of its vulnerability remains a matter of conjecture. If cyber wars are hard to imagine, high levels of 'cyber insecurity' are all too real. No one can predict where the technology might stop and there is no obvious technological plateau that would limit how disruptive cyber attacks may become. Contemporary CNIs cannot reverse their dependence on digitisation.

SHOCK AND AWE

But this is also the psychological snag for today's international terrorists. They don't want 'inconvenience' or 'disruption' – they already have that at airport security around the world. They want real destruction; death, flames, human tragedy and all the pornography of violence. They aim to shock peaceful peoples in civilised societies, not just annoy them. They want to attack transport, in the belief

www.intersec.co.uk

that it is one of society's weak spots and panic can have debilitating effects on the national economy.

So the idea of cyber bombs and city stoppers are only attractive to terror groups if they can use their cyber skills to create real violence and destruction – making trains crash, planes fall out of the sky, chemical plants blow up and so on. And it has to be clear that it was them that caused it, and that more will inevitably follow. That's a fairly tall order for even the most psychopathic of killers. Taking credit for occasional nasty accidents won't do. Terrorists can certainly maintain that more home-made bombs, stabbings, truck attacks and so on are inevitable for the foreseeable future. But they cannot easily mount a destructive CNI spectacular and simultaneously promise that there will be many more. After all, the 9/11 attacks in 2001 were certainly spectacular – but to date have not been successfully repeated or even matched.

FIGHTING BACK

And the fact is that over the last decade some societies, particularly the US, Britain, Australia, Germany, the Netherlands, some Scandinavian countries and some of the Gulf states have taken the security of key industrial control systems very seriously. In Britain, the Government identifies 13 key CNI sectors: chemicals, civil nuclear, communications, defence, emergency services, energy, finance, food, Government, health, space, transport, and water. In all cases it has sought to harden their cyber defences against external attack, though as the North Korean-sponsored criminal WannaCry virus of 2017 demonstrated, an attack designed to extort simple ransoms across 150 countries, also veered deeply into National Health Service systems to cause major disruption. There is no room for complacency. But so too, we should be realistic about what terrorist groups can achieve.

Nor should we forget that cyber is also a corresponding vulnerability for terrorists. The US' National Security Agency at Fort Meade and Britain's GCHQ at Cheltenham are, by some distance, the best in the world at cyber pursuit. That does not make them omniscient, but cyber conspiracies big enough to use CNI hacking as a weapon of violence are more likely to be detected than the myriad conspiracies that bubble away trying to incite amateur supporters to 'have a go'. Big conspiracies need some bureaucracy behind them. Indeed, Islamic State's desire to act like a proper government was part of its own undoing. US special forces repeatedly raided local headquarters, such as the swoop into Raqqa in May 2015, where a treasure trove of computer files, pen drives and print outs identified by name and function most of the individuals they subsequently went after to kill or capture.

Of course, it would be foolish not to expect terrorist groups to try to weaponise the internet rather than merely use it. The technological advantages generally move in their favour, and they have always valued novelty and surprise to keep switching the style and focus of attacks. But if, as the Chief of MI5 warned, we are alive to the likelihood and the possibilities of this new front in the terror contest we face, there is a better chance that society will be able to contain and insulate it, keep calm and carry on. ●

Professor Michael Clarke was the Director General of the Royal United Services Institute from 2007-2015. He is now the Chairman of CoJiT-UK

The 24-hour Operations Room inside GCHQ UK

Picture credit: Getty