PROTECTION FOR CRITICAL INFRASTRUCTURE

Increasing concerns about potential cyber attacks on satellites, energy installations and defence systems call for more creative threat responses, according to an expert in international security at a leading UK think-tank

The enormous growth in the processing power of computers has put great connectivity in the hands of users, but it has also offered great opportunities for cyber criminals to exploit their vulnerabilities. This has raised concerns over the privacy of digital communications and the security of personal data held on computers.

But a relatively new set of concerns is developing over the increasingly apparent links between cyber security and physical security in fields such as defence, the space industry and critical infrastructure. Dr Patricia Lewis, a research director at an independent think-tank based in London, has called for a radical review of cyber security in space to avoid potentially catastrophic attacks.

'We're looking at the moment into the cyber security of missiles and defensive systems, so many of which are now connected to the internet at some point. And we are reliant on space in our societies to a degree that many people are unaware of, but in ways that are essential to everyday life. The creation of a cyber-security regime is urgently required to develop effective threat responses.'

Dr Lewis works at the UK's Royal Institute of International Affairs – commonly known as Chatham House – whose mission is to help build a sustainably secure, prosperous and just world. A nuclear physicist by training, she is Research Director, International Security for the organisation, with responsibilities that cover all aspects of protecting humans so that they can live safe lives to the full.

Her responsibilities fall into three areas: traditional defence and security issues; societal aspects of security; and the scientific and technological aspects of security including artificial intelligence and robotics in conflict; and the scientific and technological aspects of security. The latter includes cyber security, where the challenges have grown fast since the early days of modern computers, creating opportunities for criminal activity of increasing complexity and danger to society.

'We know, for example, that criminals have been hacking into satellites; and we know they've been hacking into energy installations, including nuclear installations. This raises worries about threats to the critical infrastructure that supports utilities such as electricity, water, transport and communications. And there are similar worries about data protection – the vulnerability to attack of the large amounts of information stored on computers.

'When it comes to space, satellites play a variety of roles including providing signals for televisions and telecommunications around the world. Ships and aircraft depend on satellite global positioning and timing data for their navigation. And such data also plays a vital role in financial transactions which could be manipulated to carry out large thefts.

'The airline industry is one of the few that has been really out ahead in terms of cyber security because of worries about aircraft crashes. They have to always transmit and receive signals wherever they are, so they've been introducing authenticity checks of those the signals as part of their normal practice. Other industries need to increase the authentication of their digital information – its provenance and activity.

'This needs to be replicated in the many different sectors of critical infrastructure on which we rely – including energy, transport, food production, sanitation and banking. These are part of how we live now, but we take them for granted.'

The human-cyber interface is also important, she adds. 'Human judgment plays a vital role in these systems, and whether artificial intelligence can replace it is hard to know. But human decision-making can be a vulnerability when there are insider threats that lead to people deliberately doing things wrong, which certainly happens. And there are people who use the technology but don't understand it – another very big risk.'

'We are reliant on space in our societies to a degree that many people are unaware of, but in ways that are essential to everyday life'

Cyber threats have become a global problem, she says. And it is not just a government problem; it is also a non-state actor problem. Governments have more resources at their disposal and therefore have greater capabilities, such as having more people able to break into systems. But non-state groups can sometimes spot a vulnerability that someone else hasn't spotted. Individuals and teenage kids have done unexpected things with cyber attacks – it is not impossible for a non-state group to make quite a major gain in that respect.

All governments are involved in cyber threats, she admits – partly as a defensive measure, partly to understand what cyber attacks can do. So if they are looking at bio-terrorism for example, they have to make those pathogens to understand their impact and to work out how they can defend their countries against them. It is the same with cyber viruses: they have to make them to see what they can do.

'The best-known cyber attack on critical infrastructure was the Stuxnet worm attack on the centrifuges used by Iran to enrich uranium for nuclear fuel. This was, from all reports, a collaboration between three western powers, Israel and the United States, with some assistance from Germany. I'm sure that some other countries were involved, as well as a major corporation. It allowed them to show what they were capable of.'

At the moment, we are often protected by what Dr Lewis calls 'the wisdom of engineers'. They design things with the assumption that they will go wrong, building in resilience, backup systems and some redundancy.

Cyberattacks will keep on coming and going. We need resilience in the system so that when they occur it won't matter

So when there are cyber attacks, the resiliency of their systems means there is not always the major impact expected.

She says that this should lead us not to worry so much about cyber-attacks. 'They will keep on coming and we will keep on trying to defend against them, but some will get through. The priority should be to make sure that we have the resilience in the system so that when they occur it won't matter.

'A good example of this approach is the handling bio-terrorist threats. The one thing you can do to prevent the use of a particular pathogen is to vaccinate your population against it. The bio-terrorist can deploy the threat but if it doesn't affect people it is pointless. We need to think more like that with cyber security – if there's no impact, there's no payback for cyber terrorists.

'From other security work, we know that countering a threat with the same threat is not helpful. It just becomes an arms race: you do one thing, they do the same thing back and it carries on without end.

'We need to be smarter and more creative. If they do one thing, counter it in a completely different way that they don't expect, so they can't achieve their aim.'

She also says that talk about cyber wars is unhelpful: as with every tool of warfare, cyber will be a component of all attack and defence practices. 'People get very excited about cyber attacks and devise theories about hybrid warfare and the like. But the truth is that warfare is always mixed. It's not a football match with rules – it is war.

'We have always attacked energy systems and communications networks. If we panic and feel powerless to do anything about cyber, we'll end up paralysed. If we think about cyber as just another tool, we can deal with it.

'It's human behaviour. There's nothing new under the sun, unfortunately. We are primates. This is what we do.'●


CHATHAM HOUSE


THE COLLAPSE
SOCIALISM VANQUISHED SOCIALISM CAN LEDGER
HAVEL
Serbia Under Milošević
Milosevic
KOSOVO
PUTINISM
WALTER LAQUEUR
Caucasus Central Asia
990
INSIDE OUT
LAST EMPIRE
DECEPTION

Chatham House, London