Timothy Compston reports on the rise of state-driven cyber attacks

ON ALERT FOR STATE-SPONSORED HACKING

The involvement of states in nefarious activities, from stealing intellectual property to identifying vulnerabilities on critical infrastructure – which may be useful to exploit in a future conflict – and influencing elections – is certainly exercising people's minds right now. Of course, these sorts of state-directed actions are nothing new. The critical difference today is that cyber attacks can be initiated by individuals sitting behind a computer thousands of miles away from the victim, making the scope and scale of what is happening unprecedented and the ability to attribute blame extremely problematic.

Adam Vincent, CEO at ThreatConnect, agrees that state-sponsored hacking is now very much a mainstay of the global threat landscape and that 2017 is shaping up to be a challenging year for the security community. He points out that ThreatConnect conducted much of the cutting-edge research regarding the newsworthy breaches of 2016, including, in the lead up to the US Presidential elections, the DNC (Democratic National Committee) hack.

Vincent warns that the year ahead will witness an increase in strategic state-backed hacking among developed nations, with more poorly equipped countries jumping on the bandwagon with less sophisticated attacks: "The use of cyber espionage reached a new level of maturity in 2016. We will see an increasingly vocal response from Western governments to escalating Russian hacking activity as we begin to move towards more codified rules of cyber engagement. 2017 will still be a period of unfettered hacking activity, as state actors use aliases to mask their involvement. Organisations with any strategically useful information, whether in the public or private sector, must prepare themselves to deal with highly sophisticated phishing, infiltration and data leaking campaigns," he explains. He adds that information gathered in phishing attacks will be turned to the production of misleading or 'fake news' – something he reckons was a hallmark of the 2016 US election – designed to further a state's aims overseas.

Speaking at the RUSI second International Cyber Symposium back in October, Defence Secretary Michael Fallon said that the UK is to invest £265 million in a new Cyber Vulnerability Investigations (CVI) programme that will help the MOD better understand cyber risks. Commenting on the move, Fallon warned that: "Cyber attack is one of the greatest challenges to our security". The programme is to complement the work of the Cyber Security Operations Centre (CSOC), the £40 million facility announced in April to use state-of-the-art cyber capabilities to protect the MOD's cyberspace from malicious actors.

NATO is also redoubling its cyber security efforts, a case in point was its largest cyber defence exercise (Cyber Collation 2016) held in Estonia in December. This brought together 700 cyber defenders and legal experts, government officials and military officers, academics and industry representatives. The exercise featured a simulated cyber attack, where participants worked together to identify the threat and mitigate the impact before it could spread across national systems.

Heading across the Atlantic to catch up with PW Singer, the author of *Cybersecurity And Cyberwar* and *Ghost Fleet* – a novel of the next world war – and a strategist at New America, for his thoughts on how states are turning to the cyber domain as part of their military planning, Singer reckons that no other issue has grown more important to the 21st Century, more rapidly, affecting more people in government but also in regular civilian life, than cyber security, yet he suggests that: "There is no issue, arguably, less understood".

Singer notes that work on this area has been caught between two poles, either being framed as highly technical and tending to be focused on the hardware and software, but not dealing well with the wetware – the people side of things – or at the other end of the spectrum verging on the histrionic: "Get scared, cyber war is coming, the power grid is going down and there is nothing you can do. Give me lots of money and I will solve the problem for you".

©Getty Images

FBI Director James Comey arrives at the US Capitol for a classified briefing on Russia's involvement in the Presidential election for all members of the House of Representatives

Considering the cyber knowledge gap, Singer tells me that what he has sought to accomplish through the *Cybersecurity And Cyberwar* book, his articles and testimony to Congress, is to deliver a thoughtful, reasonable and realistic account: "I point out that there are real [cyber] threats, there are real issues and real dangers, here. They are not going away and we have to get serious about them".

Singer adds that today the cyber world permeates all facets of military operations: "The military depends on it in a fundamental manner so, for example in the US, 98 percent of military communications goes over the civilian-owned and operated internet". Alongside this, Singer explains that cyber has also become a new domain for conflict. This is evidenced, he says, by on-going activities like cyber espionage and, looking ahead, the fact that in the future 'outright war' cyber space will become a battlefield: "Cyber war is not just about the stealing of secrets, but the deployment of Stuxnet-style weaponry against military assets to take down things like GPS," he notes.

Turning his attention to recent lower-level conflicts involving a cyber dimension, Singer says: "In the war against ISIS, for example, the US military has already openly said that we are conducting offensive cyber operations against them". Commenting on events involving Ukraine and Russia, in relation to Crimea, Singer argues that Russia won the cyber part of the conflict before the physical part even began: "It owned in both virtual and physical terms the Ukrainian communication networks so when the Russians made their move in Crimea they shut down everything from Ukrainian Government and media websites to the communications of individual Ukrainian military units in the field".

One of the highest-profile examples in recent times – with hints of state involvement – relates to the use of Stuxnet malware. Designed to target industrial control systems, allegedly with the intention of disrupting Iran's nuclear facilities, Stuxnet first came to the world's attention in 2010. This was followed, over the next two years, by hacks deploying a range of computer viruses, aimed at, among other things, the Bandar Abbas electricity supply company and the Kharg Island oil

ON ALERT FOR STATE-SPONSORED HACKING

terminal – essential to the country's oil exports.

For those seeking to quantify the economic ramifications of a potential cyber attack, the *Integrated Infrastructure: Cyber Resiliency In Society* study, undertaken by the University of Cambridge's Centre for Risk Studies and Lockheed Martin, makes interesting reading. The rationale behind the study was to estimate the short and long-term economic impact of a coordinated, and sustained, cyber attack on the UK's critical infrastructure. To achieve this, researchers modelled an attack on a regional power distribution network. The scenario envisaged a cyber attack being executed by a disgruntled employee, with the backing of a nation-state, leading to the installation of rogue hardware in a minimum of 65 vulnerable substations across South-East England, triggering rolling blackouts. In the most conservative scenario, the immediate impact to the UK's economy was estimated by the report's authors as being a massive £12 billion.

Simon Ruffle, director of technology and innovation at the University of Cambridge's Centre for Risk Studies, believes there are valuable lessons to be learned from this type of study: "By better understanding and quantifying the consequences, both economic and societal, of a severe cyber hazard on our country's critical infrastructure, we underline the level of responsibility among each of the key stakeholders in this value chain". Ruffle goes on to say that through 'hyper-connectivity' we have created fantastic opportunities for smarter infrastructure use that, crucially, also bring with them a complex set of cyber risks.

Talking to Cliff Wilson, associate Partner in the IBM Security Business Unit, UK and Ireland – who is responsible for all IBM security business in the Industrial, Energy and Utilities sectors – he reiterates the concern that many industrial control systems running today were designed, manufactured and implemented before the internet came along: "In addition to being old, many of these systems can be considered highly fragile. Thus, penetration testing or other security analytical testing has to be carried out in a highly sensitive way – it is not hard to crash a legacy programmable logic controller".

Asked whether one of the problems here is that the utilities and other users are keen to have their systems more broadly connected, from a business perspective, Wilson agrees that this is an 'observable phenomenon': "A lot of old industrial control stuff is, increasingly, being connected to the internet because there is a need to be able to patch software, to pull out log data, to update software versions and also to be able to extract process data to send to corporate management systems. However, when you do that, and when you connect that piece of old equipment to the internet, it is often done in a quick and simple manner without taking security into account," he warns.

It is not just state-sponsored attempts to infiltrate and take down critical infrastructure that are cause for concern, securing intellectual property is also high on the agenda. Returning to the views of PW Singer, he is quick to highlight that in the last Cold War the internet simply didn't exist: "Today if you are looking at a scenario of NATO vs Russia or US vs China, there are crucial cyber security and cyber warfare elements to it".

One of the challenges for the US or China in an arms race, stresses Singer, is the ability to secure intellectual property: "It is very hard to win an arms race when you are paying the research and development costs of the other side". Singer illustrates this point by referencing the Joint Strike Fighter, the F35: "This is the most expensive weapons project in the whole of human history. The US and its allies will spend over $1 trillion on this programme". Unfortunately, Singer says that the F35 design has been hacked on at least three different occasions: "That is why the Royal Navy doesn't have F35s yet and China is already flying its J31, which is essentially a clone".

To conclude, in today's world – where connectivity is the order of the day – the potential for cyber attacks by state actors has never been greater and, as result, there is a pressing need for countries and organisations in the firing line to shore-up their defences. Matt Little, an encryption expert at US cyber security vendor PKWARE, agrees that the threats are not going away any time soon: "We will continue to be attacked by hostile nations, terrorists and criminals, and they will continue to exploit how vulnerable we are. Before Trump won the election, the [US] Government proved time and time again that it is not capable of protecting its citizens or even itself from cyber attacks". Little's message to the new Trump administration is that it needs to do the one thing that a Government is capable of doing: updating regulation to allow private corporations to better protect themselves, even if these updates make it more difficult for the intelligence community to function: "The private sector should be incentivised to engage in active defence measures".

Timothy Compston is a journalist and PR professional who specialises in security issues. He studied International Relations and Strategic Studies at Lancaster University, is PR director at Compston PR and a previous chairman of both the National PR Committee and CCTV PR Committee of the British Security Industry Association (BSIA).