INTERNET WAR ZONE

Picture credit: Getty

Sony had to cancel the Christmas launch of its movie *The Interview* following a massive cyber attack believed to have been from North Korea

Anthony Tucker-Jones *talks to Ian Goslin Managing Director, Airbus CyberSecurity, UK about the mounting cyber threats to NATO*

ATJ: Ian please very briefly tell our readers about your role with Airbus and your background.
IG: I joined Airbus in 2012 and now head up the UK arm of Airbus CyberSecurity. Before that, I served in the Royal Air Force for 28 years as an engineer officer, where much of my focus was on ensuring the availability and security of military communication networks across the globe, including in Afghanistan and the Middle East.

ATJ: What sort of services does Airbus CyberSecurity offer?
IG: Airbus CyberSecurity provides companies, critical national infrastructures and government and defence organisations with reliable, high-performance products and services to detect, analyse and respond to increasingly sophisticated cyber attacks. We provide services including high-grade cryptography and key management, domain gateway protection, threat intelligence capabilities and full spectrum cyber protection services. We are primarily based in the UK, Germany and France, with an additional presence in Spain, the Middle East and the US.

ATJ: Tell us a little more about your European Cyber defence centres and the important work that they conduct?
IG: We operate individual Security Operations Centres in each of our three core markets, offering managed security services to external customers. Each country has its own strengths – the UK has a lead in terms of high-end cryptography, France is focused primarily in developing new cyber security solutions and Germany is known for its work in Secure Network Gateways.

ATJ: What categories of hacker do you typically come across?
IG: We encounter all types of hackers. These include nation state actors, who are usually driven by a government policy or directive; criminal groups, who are largely motivated by financial gain and hacktivist groups, who are mostly concerned with promoting a political agenda. Threats are becoming richer and more mature, but it is usually the simple exploitation of poor cyber hygiene that results in the greatest threats to the general public.

ATJ: Data disruption and data theft are now a major problem – do you think the general public is aware of quite how extensive the threat is?
IG: Data theft is now established in the public consciousness, although the concept of data corruption is less well understood. Overall, the greatest problem with awareness of cyber threats is the mentality of "it won't happen to me". We need people to realise that it could be them, and it could happen tomorrow.

ATJ: What was your first reaction to the recent highly publicised WannaCry ransomware attack?
IG: This incident underlines the importance of basic cyber hygiene such as updating software and training employees to spot phishing attempts, as well as consistently monitoring the assets and responding to incidents. Employees should be extremely wary of unexpected emails, particularly if they contain links or attachments, because email is usually one of the main infection methods.

ATJ: There does not seem to be a day that goes by without reports of hacking. Is the situation getting worse or is it just a case that governments and businesses are constantly playing catch up?
IG: The truth is, there are always new reports of hacking, but we tend not to hear about the much larger number of attacks that are successfully stopped. But rather than focusing on the attacks themselves, we should be focusing on how quickly we respond, stop, block and recover from attacks. It's the speed of our response that matters. It's naïve to believe that we will always be one step ahead – for example, when zero-day attacks are launched, they take advantage of new vulnerabilities that haven't yet been reported, so they usually have some initial effect before they are spotted and dealt with; the trick is to identify early and respond quickly, thereby minimising the impact.

ATJ: Following Brexit, these have been uncertain times for Europe, from your perspective was NATO being alarmist last year when it declared the internet a war zone?
IG: There is no doubt that the internet and cyber space are becoming primary areas of conflict and a place where advantage can be gained or lost, depending on your security posture. So I don't think that the declaration was alarmist – it just reinforces the fact that the internet is a tactical area where we need to win advantage. However, the internet has furthered our society and economy in so many ways, it's important for us to focus on the many benefits it affords, rather than just viewing it as part of the theatre of war.

ATJ: NATO talks of cyber warfare playing a role in future global conflicts, is this the alliance's way of acknowledging that it needs to develop the infrastructure and strategy for fighting a cyber war?
IG: Cyber warfare is definitely an area where governments are looking to gain an advantage, and it's true that NATO and individual governments all have a role to play in making each nation within the alliance cyber secure. But when it comes to our infrastructure and strategy, we need to look beyond the military machine and focus on having a cyber secure environment within each function of society and the economy. This is because tomorrow's cyber warfare could target not just military infrastructure, but our broader society with attacks seeking to disrupt our critical national infrastructure, banks or industries.

ATJ: Do you feel that NATO has been too slow in responding to the growing threat of state-sponsored hacking?
IG: NATO is made up of a variety of different, individual nations, all of whom are at varying stages of cyber security knowledge and defences. The fact that it has raised the issue, and is taking proactive action, is a positive step. The very nature of NATO, as a coalition that shares intelligence and understanding between member states, will allow all nations involved to quickly reach a higher standard.

> THE SIMPLE EXPLOITATION OF POOR CYBER HYGIENE USUALLY RESULTS IN THE GREATEST THREAT

ATJ: Do you think the cyber attack on NATO member Estonia back in 2007 was a key turning point for the organisation?
IG: The attack on Estonia was certainly an important wake-up call. Since the attack, Estonia has responded particularly well and is now one of the leading NATO nations in terms of cyber defence. Of course, the attacks also prompted NATO to enhance its cyber war capabilities and to establish the alliance's cyber defence research centre in Tallinn in 2008.

ATJ: Why has NATO been so slow to respond to the cyber threat?
IG: The cyber security industry as a whole is incredibly fast moving, and organisations in every sector across the world can struggle to keep up because the threats change so rapidly. For example, just to protect against the vulnerabilities that have already been disclosed within existing software requires emergency updates (patches) to be installed almost constantly.

ATJ: In your view, what are the key cyber threats NATO needs to protect itself against?
IG: The actual threats are similar to those experienced

by commercial companies – but rather than affecting company revenue or customer data, these attacks could afford a tactical advantage within a military context. For example, a Distributed Denial of Service (DDoS) attack could be used by state-sponsored attackers against a military force, to flood its network with so much traffic that it overloads the system. Similarly, a military force's ability to command and control could be affected by information theft or information corruption, which could slow down its decision cycle and erode trust in the information being circulated. This can be particularly damaging, because as anybody in the military sphere already knows, staying ahead of your enemy's OODA loop (the decision cycle of observe, orient, decide and act) is one of the most important strategies of all.

ATJ: Traditionally NATO has been about boots on the ground protecting Western Europe, though having operated in the Balkans and Afghanistan. Can NATO adapt in a timely manner to fight on this new virtual battlefield?
IG: The strength of NATO comes from the fact that it is an alliance made up of individual military forces. Some of the individual forces are among the most cyber capable in the world, so by sharing this expertise and intelligence it will definitely be able to operate and dominate as we move further towards operations in the cyber domain.

ATJ: How can Airbus CyberSecurity help NATO and what do you think are the critical elements in shaping their new strategy?
IG: To strengthen NATO, each individual nation needs to be cyber resilient so that its military efforts are not undermined by an attack on the economic welfare of any individual state. Regardless of whether attacks are orchestrated by a bedroom hacker, a hacktivist network or a nation state, countries need to ensure that each element of their society – be it critical national infrastructure, banks or individual industries – has a strong cyber security posture. Airbus CyberSecurity can help UK industry to strengthen its defences against these types of threats.

ATJ: What lessons can be learned from the cyber attack on Sony in 2014, the US Office of Personnel Management hack in 2015 and indeed the US elections last year?
IG: These high-profile attacks remind us that, should a state actor or group of hactivists choose to influence world events, they have the potential to do so. Whether the source of attacks or exact course of events is ever proved, the damage is often done just by reputational impact. Any organisation – whether blue-chip multinational, government department or the military – can be vulnerable to cyber attacks if the right level of cyber defence is not put in place.

ATJ: You recently warned that cyber attacks directed at critical infrastructure can be economically damaging. We recently saw with the NHS that it can also put patients' lives at risk. Are we going to see a new breed of hacker that deliberately endangers people?
IG: It's extremely difficult to speculate about hackers' motivations, because when attacks are launched in the wild, the perpetrators don't always realise what the outcome will be. The recent WannaCry attacks demonstrate how all sorts of organisations can get caught up as collateral damage, regardless of who may have been the intended victim. So how this plays out in the future will likely be a combination of individual attacker's motivations and the collateral damage of different attacks.

ATJ: You have warned that utilities such as power, water and transport could be at the mercy of the hackers. Will hacking be the permanent downside of the internet?
IG: There will always be people trying to corrupt and bend the internet to their needs. But across all sectors, in industry and commerce, people are becoming more aware of the threats involved, which is a vital first step to improving a security posture. So I have great optimism that the situation will improve and our response times will get better ●

Anthony Tucker-Jones is *intersec*'s Terrorism and Security Correspondent. He is a former defence intelligence officer and is now a widely published defence commentator specialising in regional conflicts and counter terrorism.

Picture credit: Getty

The global ransomware cyber attack hit more than 200,000 victims in more than 150 countries