CYBER DEFENCE

BT's Network Control Centre at Oswestry

Anthony Tucker-Jones *concludes his interview with Kevin Woollard, Operations Director BT Research & Technology, discussing the latest developments in cyber security*

ATJ: How much has the Ministry of Defence's budget cuts affected BT's R&D work in this particular field?
KW: Our aim is to help the MoD introduce new technology innovations quicker – helping them to reduce the overall cost of their IT programme. We can do this by taking solutions, which provide benefits in other sectors and adapting them to suit the requirements of the defence sector.

ATJ: Are you having to dovetail military R&D into civil applications?
KW: This question probably isn't applicable to BT as we specialise in technology R&D rather than military R&D.

ATJ: Defence requirements are always a moveable feast can you tell us about current priorities for the defence and security sectors?
KW: Cyber defence is a priority, as you would expect. As is the need to reduce the size, weight and power of the technology equipment that needs to be shipped around the world, together with increased collaboration and connectivity in remote locations. Cloud services, software defined networks, wire-free technology, mobility solutions – all with a high level of network protection – are just some of the key focus areas.

ATJ: Does BT conduct R&D for the Home Office in terms of counter terrorism applications? If so, within the constraints of operational security what areas have been explored?
KW: We're not in a position to comment on this.

ATJ: Telecoms is now a very fractured market, what does BT do to keep ahead of the competition in terms of innovation and safeguarding clients?

KW: BT is exceptionally well placed to ensure that it continues to lead the pack when it comes to spearheading innovation and major technological breakthroughs. We currently invest around £500m per annum in R&D making BT one of the largest investors in R&D of any company in the UK and globally in the telecoms sector. The business currently holds an impressive 4,560 patents; indeed, recent figures from the European Patent Office revealed that BT ranked fourth for the most patent applications made by UK companies last year, just behind Rolls Royce, Unilever and BAE.

In terms of our security credentials, BT also comes from a position of strength. We employ more than 2,500 security professionals around the globe, making BT one of the largest dedicated security and business continuity practices in the world. We're uniquely placed to help protect businesses and organisations from the growing, global nature of cyber threats. Our global network gives us a ringside view of the global threat landscape and provides our customers with a first-hand and real-time view of emerging threats.

What's more, we don't just protect customers' and BT's own infrastructure, but also the UK's critical national infrastructure. Other countries are also starting to entrust the security of their critical national infrastructure to BT too. BT provides managed security services to 6,500 customers worldwide, including both FTSE100 and Fortune 500 companies – so the calibre of our security clients speaks volumes.

ATJ: Do you feel that cyber crime can ever be truly thwarted or is it a case of ongoing protective measures and vigilance?
KW: No single IT and network security provider can ever offer a business or organisation a 100 percent guarantee that their network and critical data will be kept safe from attack. The tools and techniques being deployed by hackers around the world to penetrate networks are evolving all the time, while the volume of attacks continues to grow exponentially.

That's why we have 14 Security Operation Centres (SoCs) around the globe, which monitor BT and our customers' networks and systems 24/7, 365 days a year. Our teams constantly monitor the threat landscape and flag potential threats and issues so that action can be taken to prevent them.

Furthermore, we're now combining and analysing Big Data from our global network on our cyber platform to spot and mitigate even slightly abnormal activity significantly in advance of cyber attacks.

ATJ: Network protection in the face of unauthorised access is a major problem. Cloud, Firewall, Mobile and Web security are all a headache for businesses and governments. As there is no one-size-fits-all solution, how do you see this field developing?
KW: BT is able to call upon a network of nearly 8,000 security consultants and partners, such as Darktrace, Cisco, Palo Alto and Fortinet, to ensure that our operations and solutions deliver the best possible results for customers.

The strategic partnerships that we've forged with leading security vendors across the globe means that we're able to address the entire range of customers' needs – from antivirus and parental controls to protect families in their home, through to complex managed security solutions used by businesses, banks and national governments.

ATJ: An enormous proportion of large companies are under threat of disruptive digital crime – surely the same goes for government and critical infrastructure?
KW: Absolutely, and we can see the emphasis that the UK Government is placing on the scale and nature of the threat with the launch of its National Cyber Security strategy last year.

This strategy provides a comprehensive approach to securing the country's critical communications infrastructure and will see the Government take action to strengthen automated defences and make it more difficult for criminals to exploit the internet to their advantage.

CYBER ATTACKS ARE GETTING BIGGER, MORE COORDINATED AND MORE SOPHISTICATED

ATJ: Is BT playing its part in this process?
KW: We at BT are stepping up too in supporting the Government's strategy. We will do this by strengthening internet protocols to make it more difficult for UK machines to participate in a DDoS (distributed denial of service) attack, blocking malware sites to protect our customers, and making it more difficult for hackers to spoof email addresses and con victims into thinking they've been contacted by a legitimate organisation.

ATJ: Just how secure would you say cloud-based services are?
KW: Because cloud computing operates in a virtual environment, the threats that apply in the virtual world apply in the cloud — the so-called web of vulnerability. As cloud computing expands, so does the landscape of threat, and the growing range of mobile devices we have at our disposal are the carriers of risk. The keys to protection are impeccable vigilance, forensic data protection and robustly shared responsibility; delivery is the domain of the communications provider while usage is your responsibility.

ATJ: What are the latest developments in cloud security?
KW: BT's researchers and practitioners are very active in cloud security initiatives and have developed an 'industrial-strength' SaaS (software as a service) solution. It's highly secure and, because BT controls both the data centres and the network that connects them to its customers' premises, performance can be tightly controlled. Organisations no longer face the risk that enhancements to networks, applications or

Picture credit: BT

servers will simply move bottlenecks elsewhere.

ATJ: In your view is cyber crime and cyber warfare essentially the same beast or should they be treated completely differently?
KW: Cyber warfare has transformed the definition of data and security. The worrying trend is that these attacks are getting bigger, more coordinated and more sophisticated, with the motivation shifting from simple fraud, to a desire to disrupt or destroy whole infrastructures. Attacks are becoming better at breaching security defences, causing major disruption and even bringing down systems

BT IS ONE OF THE LARGEST INVESTORS IN R&D IN THE UK AND GLOBALLY IN THE TELECOMS SECTOR

for a number of days. The term cyber warfare is typically used, however, to describe large-scale state-sponsored attacks or terrorist activity where malicious organisations or individuals use computer systems to cause physical or financial damage and disruption in order to intimidate or coerce governments for political or social reasons.

When we think of cyber crime, we usually mean organised crime involving criminal groups using computer systems to commit crimes such as extortion, money laundering, scams, credit card forgery, identity theft and other online fraud.

State-sponsored attacks are increasingly hitting the headlines worldwide. Due to the potential impact on critical communications infrastructure and the wider political system, you could argue that the gravity of the threat deserves to be considered in a different light to the threat posed by the more opportunistic cyber criminal activity that we see on a daily basis.

ATJ: So in essence it's an evolutionary process?
KW: In truth, the problem is best thought of as a continuum from petty crime up to cyber warfare and the boundaries are and will be blurred, requiring a sophisticated set of defences that will need to be deployed as required. Increasingly, it will be essential that strong collaboration is established between industry, law enforcement and government agencies such as the National Cyber Security Centre (NCSC).

ATJ: How do you see the web developing in the future – social media seems to be the main visible imperative, what are the real drivers pushing future apps?
KW: The web has become central to every individual and every business and their daily activity. However, it is without doubt a genie that now out, will never want to go back into the bottle. We are beginning to see the first rumblings of discomfort about the future of the internet, driven largely by security concerns, both personal, industrial and national. Sir Tim Berners-Lee (inventor of the world wide web) has identified concerns related to privacy that he feels need fixing, at the same time Google, Facebook and Twitter faced questions from the Home Affairs Committee about online hate crime and harassment and, of course, the rise in fake news being delivered online to a purpose that is difficult to pin down. Against this, we are beginning to connect more and more devices to the internet as we instrument the world we live in.

ATJ: Will this connectivity not further complicate the online security problems?
KW: While we fully expect this 'Internet of Things' to transform the way we manage the world, it will provide a new set of devices for attack and misdirection that will require a redoubling of our efforts to protect our data, our networks and our apps and services ●

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.

Fake news is becomingly an increasingly thorny issue

Picture credit: Getty