[COLUMNIST] TREVOR BINGHAM, BUSINESS DEVELOPMENT MANAGER AT IT SPECIALISTS, FUEL

THE WAR AGAINST CYBER CRIMINALS

WITH THE RECENT JOINT ANNOUNCEMENT FROM PRIME MINISTER DAVID CAMERON AND US PRESIDENT BARACK OBAMA THAT THEY ARE TO LAUNCH A SERIES OF JOINT CYBER 'WAR GAMES' AS A PART OF A WIDER MOVE TO COORDINATE ANTI-HACKING EFFORTS, **TREVOR BINGHAM** INVESTIGATES THE BACKGROUND TO THIS DARK WORLD.

The high-profile cyber attacks and hacks of the past year have seen western governments shining a spotlight on cyber security. Attackers believed to be from North Korea hacked into Sony Pictures Entertainment at the end of 2014, stealing vast amounts of data and intellectual property.

As President Obama emphasised in a recent speech: "No foreign nation, no hacker, should be able to shut down our networks, steal our trade secrets, or invade the privacy of American families, especially our kids."

While the high-profile attacks were targeted in the US at some of its best known companies like Sony and eBay, these cyber criminals often base their attacks on creating maximum damage ignoring national borders.

It's reported that plans are being drawn up to simulate an attack on London's financial sector which is closely linked to Wall St in the US. The plan agreed by David Cameron and Barack Obama will also see the creation of specialist cooperative 'cyber cells' operated by the UK and the US. The UK and US have always focussed heavily on cyber security but they now see the need to combine their efforts to further improve their cyber defences.

Both governments insist that this isn't only about protecting companies, it's about protecting people's data and personal finances, as often these attacks can have real consequences for people's prosperity and livelihoods.

The latest initiative follows wider attempts by the UK government, as part of the Cyber Security Strategy launched in 2011, to bolster the nation's cyber defences and increase the sharing of the threat of moving data between the public and private sectors. The revived UK Strategy has launched several key initiatives since being announced, including the Cyber Security Information Partnership, the UK Computer Emergency Response Team and the soon to launch Cyber Insurance scheme.

However, this bolstered cyber security initiative has a secondary focus for the UK government – to set up the UK as a global exporter of cyber security solutions. Defence and security exports, including cyber security, play an important part in strengthening the UK economy, supporting jobs and supporting the defence of the countries we do business with. The UK Trade and Investment department's Defence and Security Organisation will do its best to ensure that major multinational companies based in the UK are given every support to remain secure and in turn will also help drive the huge export potential of the UK security sector in which Northern Ireland plays a significant part.

Security researchers have already uncovered a wave of fresh threats this year, including the defence-dodging 'Skeleton Key' malware and the advanced 'Cryptowall 3.0' ransomware.

Prior to the announcement, many privacy groups had expressed concerns about close ties and coordination between GCHQ in the UK and the US National Security Agency during the PRISM campaign. This campaign saw the US government siphon off web user data from technology firms including Google, Apple, Facebook, Twitter and Yahoo. GCHQ is known to have used some PRISM data during its operations.

The Intelligence and Security Committee ruled in July 2013 that GCHQ's use of PRISM data was entirely legal and after recent attacks the appetite to dispute this practice may have shrunk somewhat.

Other uses ways of using collective and less intrusive data is to analyse behavioural movements and activity to predict traditional crime.

Many of our larger enterprises are turning to super-fast analytics and monitoring solutions like that of HANA, a high performance database to combat the predicted cyber threats facing them on a daily basis which reminds me of the old adage – forewarned is forearmed! The increased number of potential attack avenues open to hackers means that companies can no longer rely on perimeter defences – a sort of 'war games' on a multinational company platform!

This new security-monitoring application collects all significant hardware, network and software vendors' security messages from companies like Microsoft, HP, IBM, CISCO and Oracle into a large HANA database and does multi-system security breach analysis.

The software is becoming more essential because it's no longer the case that hackers break into one system and stop. They go into one system and from there they go into another system and then to another system – the thieves are not going through the main door anymore, they're coming through the basement, or from behind.

So as 2014 is often referred to as 'The Year of The Hack', will 2015 be 'The Year of Cyber Security'?

Let's hope so!

"SECURITY RESEARCHERS HAVE ALREADY UNCOVERED A WAVE OF FRESH THREATS THIS YEAR, INCLUDING THE DEFENCE-DODGING 'SKELETON KEY' MALWARE AND THE ADVANCED 'CRYPTOWALL 3.0' RANSOMWARE".