SPY WARS

Tony Kingham *reports on the fight back against espionage*

On almost any given day it is easy to find a story in the press reporting various types of cyber crime, cyber espionage or even cyber warfare. Whether it is a criminally inspired attack like the WannaCry ransomware attack in May 2017 – which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency – or a politically motivated espionage such as that recently reported in the *Wall Street Journal* when: "hackers working for the Russian Government stole details of how the US penetrates foreign computer networks and defends against cyber attacks after a National Security Agency contractor removed the highly classified material and put it on his home computer, according to multiple people with knowledge of the matter. The breach is considered the most serious in years, could enable Russia to evade NSA surveillance and more easily infiltrate US networks."

It is easy to see why cyber crime and espionage are so attractive to criminals and governments alike. After all, most of our most valuable information is stored somewhere on a computer and if you can get at it, the crime of taking it is as near risk free as it can be, especially if you are protected by a national border.

CHANGING FACE OF CRIME

I read an interesting fact recently that incidents of armed robbery in London, of the sort that used to involve a sawn-off shotgun and a pair of ladies' tights, is almost a thing of the past. Incidents have dropped by around 90+ percent since it's heyday in the seventies. Now, this will be partly due to the number of CCTV camera's in London and maybe partly due to the sheer volume of traffic making a getaway in a fast car almost impossible – but a major factor is that for the modern-day villain it is far easier, safer and potentially more profitable to engage some young geek to hack a bank's data or commit online fraud than it is to run the risk of a 25-year sentence for armed robbery. A former Scotland Yard detective has told me that Scotland Yard doesn't even investigate frauds under £50k because of "lack of resources" and the perpetrators know this.

So, unless you have lived in a cave for the past five years, most people are aware of the cyber threats and this is especially true among government and corporate circles.

What is not so widely understood, is that old-fashioned human spying by people from inside and outside an organisation, is still a very real threat and why that threat is set to continue.

Hackers are often able to collect huge amounts of data, but that in itself creates a problem. Sifting and interpreting data, while easier than it once was, means that important things may be missed and doesn't necessarily interpret that data.

A well-informed and well-placed insider may be able to access information that has not been hackable because for example it is "air gap" protected. But also, crucially because they can provide context for the information that they pass.

For instance, the purchase of a new type of circuit board for a mechanical system may go unnoticed, but that change of circuit board may be critical to the proper functioning of a crucial system.

LOOSE LIPS SINK SHIPS

Human spies are also able to provide information that is not necessarily held in any database. Like gossip about the member of the team who may have financial or marital problems that leave them vulnerable to blackmail or coercion. Private conversations in the board room, on the phone or in the office kitchen. Conversations, opinions and ideas which may impact on the outcome of a given set of circumstances whether that's on a political, financial or national security issue.

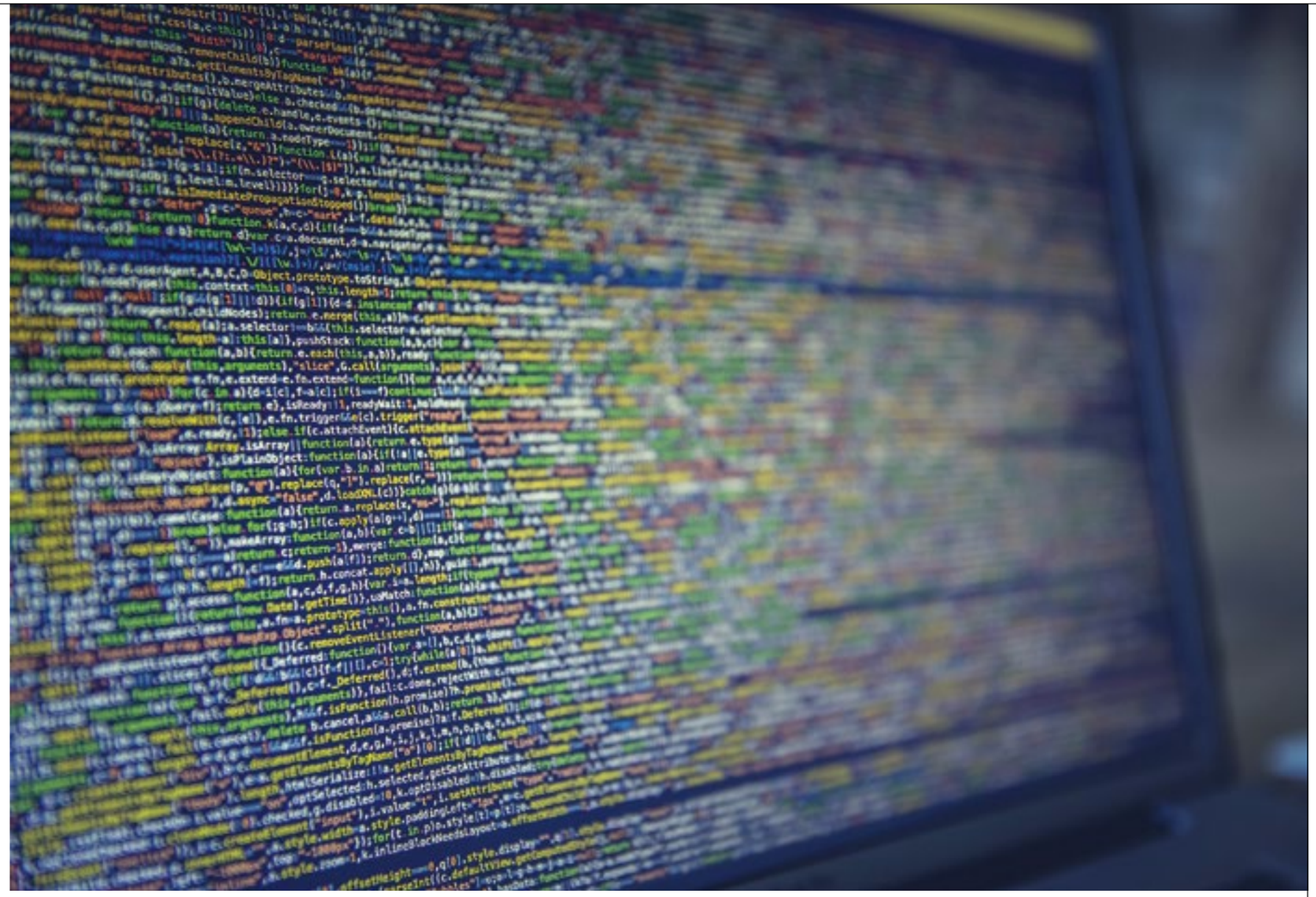
> **SURVEILLANCE TOOLS CAN NOW BE HIDDEN IN AN ENORMOUS VARIETY OF HOUSEHOLD GOODS**

Earlier this year, it was reported in the UK *Guardian* newspaper that a 65-year-old woman working as a contractor for a UK Government department was arrested by UK anti-terrorism police on suspicion of an offence under the Official Secrets Act, which covers espionage and passing secrets to an enemy. In this case most likely Russia or China.

In the US, in June 2017, Kevin Patrick Mallory was arrested and charged under the Espionage Act on charges of performing espionage on behalf of the Chinese Government. Mallory was allegedly given special devices for communicating documents to Chinese intelligence agents, including those classified as Top Secret.

Russia and China are extremely active against the West and *vice-versa*. The Chinese claim to have killed or imprisoned between 18 and 20 CIA sources since 2010 dismantling a spy network that will have taken years to develop. Or at least, that is what is reported.

And it is not just the usual suspects. According to a report on the *Chinese Global Times* website: a Japanese man arrested in North-East China's Liaoning Province was caught engaging in spying activities. Chinese experts said: "Japan is a nation of spies that has long engaged in economic espionage across the world, but their main mission in China is collecting military-related data."



Cyber espionage is becoming an increasingly popular means of attack

At least 12 Japanese men have been detained in China on suspicion of engaging in espionage since 2015, four of whom were released and returned to Japan in July. Five were prosecuted and the remaining eight remain in custody, Japanese media *Kyodo News* has reported.

TRADE SECRETS

It is not just state secrets that spies are after. Seven people were arrested in the US for conspiring to steal trade secrets of a "syntactic foam" product, which can be used for an array of purposes ranging from stealth technology to oil exploration. Federal officials arrested six people including four US citizens and one Chinese national, and charged another person who works for a Chinese manufacturing firm.

In the Netherlands in April 2017, it was reported that a Dutch employee of the German industrial giant, Siemens, was arrested for alleged spying for trade secrets, once again for the Chinese.

Technological advances have made spying cheap and easy, which means almost anyone can become a spy if they have the right political or financial motivation. This is especially true of GSM technology. Surveillance tools can now be hidden in an enormous variety of household goods like phones, power strips, light bulbs, alarm clocks, digital music players, power adaptors, smoke detectors and many more.

Using your GSM phone, you can call into your surveillance device from anywhere and conduct covert room monitoring without anyone knowing. You can hear and record all conversations within range and when you're finished simply hang up.

Many of these devices have covert 3G cameras installed that allows the operator to transmit clear video footage to any 3G video mobile phone anywhere in the world. Some have motion sensors that activate when someone enters the room, ideal for the boardroom or meeting rooms.

All organisations are potentially vulnerable, whether that's from a politically motivated, avaricious or disgruntled employee, contract workers or maybe even the photo copier repair man or woman. Anyone that has access to your building can leave a device and leave you vulnerable to surveillance. So, what can be done?

Gerry Hall, Managing Director of International Procurement Services has been working with government agencies, international companies and high net worth individuals supplying security solutions, debugging sweep team services, countermeasures and consultancy for more than 25 years.

"No organisation can ever be totally secure, especially when people are coming and going, but it is important to set out your security priorities and establish protocols.

SETTING PROTOCOLS

"For instance, defining and documenting what sort of information constitutes sensitive and secret and lays out where, when and in what context discussions about this information should be had. This includes rules about telephone conversations on both landlines and mobiles. These protocols should be made available to all members of staff, regularly updated and staff should sign off on that the information is read and understood.

"It could be argued that all internal information within an organisation is proprietary and therefore sensitive and secret, but it is just good sense to make special consideration for high value information and make everyone legitimately involved aware of the special rules that apply to it.

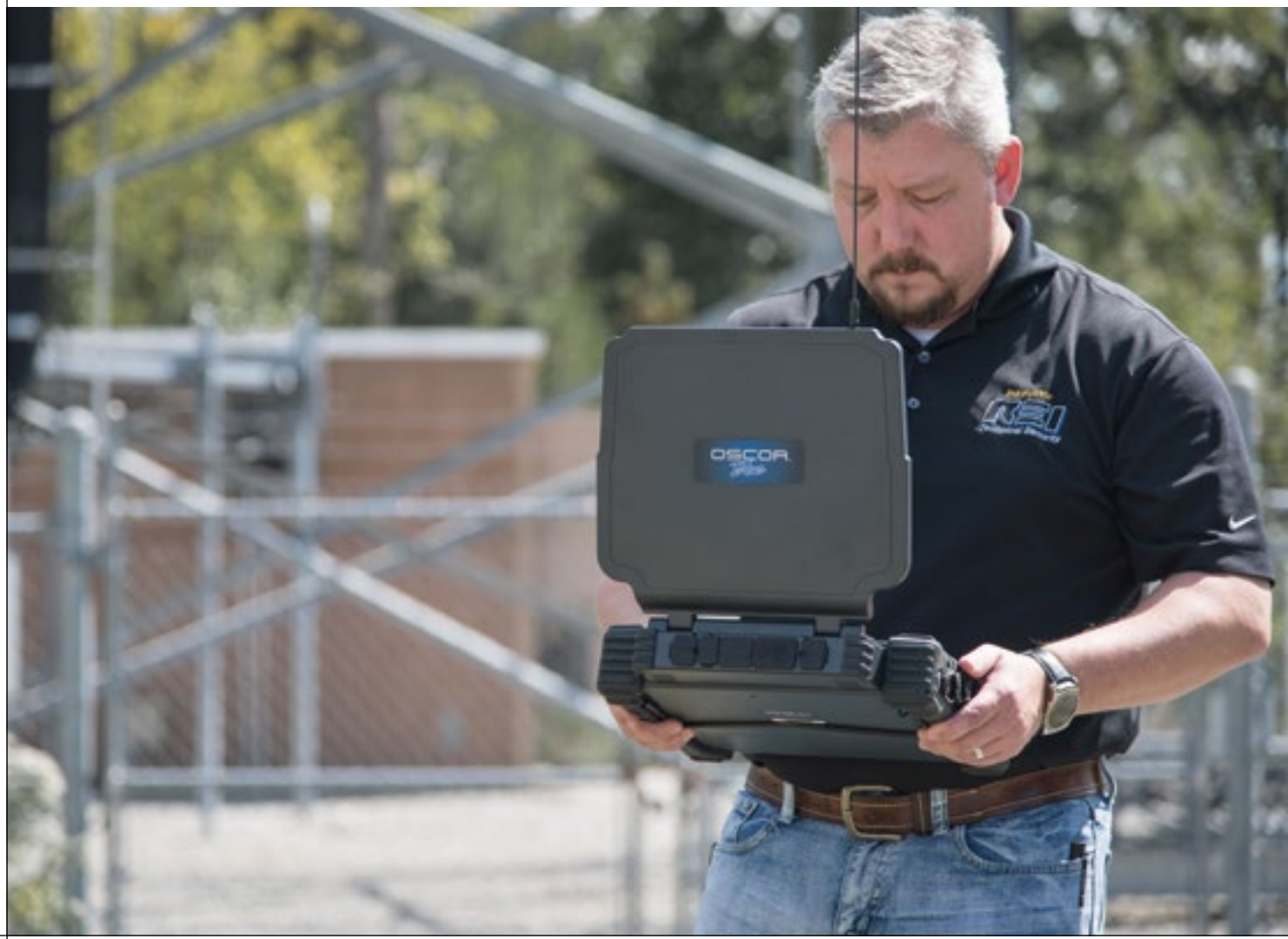
"Practical measures that can be taken include establishing secure areas, which are the only designated spaces where discussion of sensitive and secret information is allowed. These can be permanent, such as the boardroom or CEO's office or temporary such as a hotel room. These areas must be swept for devices on a regular basis to ensure that they are clear and free of surveillance. And not just for the designated spaces, but also any phone lines.

"Now you can do this internally by specially trained members of your own staff, but they must be properly trained, and have the right equipment, which is expensive. As a guideline the minimum equipment requirement would include a Non-linear Junction Detector together with a dedicated TSCM Spectrum Analyzer such as the Oscor Green, Thermal Imager *etc*. Realistically an investment anywhere between £50,000 and a £150,000.

> **IT IS EASY TO SEE WHY ESPIONAGE IS SO ATTRACTIVE TO CRIMINALS AND GOVERNMENTS**

"The alternative is to engage a company like ours that provides specialist sweep teams with all the right equipment, training and experience. We've carried out thousands of sweeps for hundreds of commercial organisations and government agencies worldwide. But beware, if your sweep team does not have the right equipment you will be wasting money and could be compromising your security"

Tony Kingham is a freelance journalist and publisher of www.WorldSecurity-index.com, specialising in information and public relations within the defence and security markets.



Regular security sweeps for hidden devices is a vital consideration

Picture credit: International Procurement Services