A new age of espionage

Electronic spycraft is getting easier but more controversial. The old-style human sort is getting harder but more useful

Aug 1st 2015 | From the print edition

CYBER-CAFÉS were once a favoured tool of Western intelligence and security agencies. They were inconspicuous, cheap to establish and highly effective. Set up near an international summit buzzing with targets, or close to a mosque favoured by Islamist extremists, these facilities allowed their masters to monitor browsing habits, obtain targets' logins and passwords, and plant spyware for future use. This was legal: consent was buried in the terms and conditions which users clicked on without reading. And in a neat twist, security-conscious people trying to avoid using their own computers favoured such places. Some would hop between cafés, unaware that all the convenient ones were run by the authorities.

Not anymore. Edward Snowden, a fugitive former contractor for America's National Security Agency (NSA) now living in Moscow, revealed the use of cyber-cafés to spy on the G20 summit in London in 2009. Now people are wary. In many countries the cyber-cafés have been closed. The staff who ran them have had to be moved (and in some cases given costly new identities). As a result, keeping track of terrorism suspects is now harder, spooks say.

The episode highlights one of the most important trends in modern intelligence work. Collecting electronic information is generally getting easier. It is hard to lead a completely non-digital life, and any activity using computers and networks creates openings for the watchers. An e-mail is as easy to read as a postcard for anyone with modest technical skills. With a few tweaks, mobile phones become tracking beacons and bugging devices. Most people readily trade private information for convenience. And hacking into computers can yield vast amounts of intelligence.

A lot of spying, however, has become trickier. It is much more difficult for intelligence officers to maintain secrecy and create fake identities. And high expectations of privacy, especially in the digital realm, mean that in many countries the work of intelligence and security agencies arouses outrage, not gratitude.

Secrets and lies

In theory it should come as no surprise that spy agencies spy, and that the biggest and best are good at it. But the Snowden revelations underlined some uncomfortable facts. Espionage is inherently lawless. Supposedly private communications are fair game. Seemingly friendly countries spy on each other. The news (subsequently dismissed by German prosecutors) that America listened to Angela Merkel's mobile phone was one of a corrosive series of revelations which led to the CIA station chief's expulsion from Berlin—a low point in the two countries' relations.

In particular, electronic intelligence-gathering is based on trawling and sifting huge amounts of information. This includes private communications between people who have no connection to crime, terrorism or statecraft. Western spymasters insist that this material is of no interest to them: it is merely the inevitable by-product of collecting communications which contain the material they are interested in. In some countries the public seems unworried. A sweeping new spy law has caused few ripples in France, for example. In others, such as Germany, spooked by its Nazi and Stasi past, it has led to blazing rows. Whose information may be intercepted? Where should it be warehoused? For how long? Who should have access to it? These questions go to the heart of the relationship between the state and the citizen.

Both Britain and America are rejigging their oversight arrangements in an attempt to assuage public worries. America's NSA no longer directly intercepts and stores electronic communications between residents of the United States: it must apply for a warrant to obtain them from internet and phone firms (access to foreigners' communications remains unaffected). Britain's independent scrutineer of terrorism legislation, David Anderson, a lawyer, has issued a report blasting what he terms ramshackle supervisory arrangements. He wants stronger judicial scrutiny instead of the existing system, which is based on government ministers authorising intercepts.

Though the spy agencies remain incandescently angry with Mr Snowden and his supporters, spymasters in Britain and America grudgingly admit that they now need to work to regain public trust. The old combination of secrecy and public ignorance is no longer enough. Spies now need a public consensus to legitimise their work—especially

when it comes to activities which intrude on the privacy of their own citizens. Building that will take years.

The Snowden revelations not only showed that electronic espionage was far more intrusive than many had realised. They also gave clues about how to avoid it. Encrypted electronic messaging, for example, is much tougher to intercept and trawl for clues than e-mails or phone calls. The encryption keys may be held only by the communicating parties—so there is no point in serving a warrant on, say, Apple to get access to messaging that uses its platform. The spooks complain mightily about this—James Comey, the director of the FBI, says firms which provide encryption software to their customers should have a duty to provide the decryption keys to law-enforcement agencies. Critics see this as either futile or dangerous: a warehouse full of keys would be a target for attack.

What the spooks talk about less is the many ways in which they can get round encryption. However heavily encoded a communication is while in transit, it must be composed and displayed in a way that humans can understand. This involves keyboards and computer screens—known as "end-point vulnerabilities". If you know what your target has written, and what he is reading, the fact that it was transmitted with heavy encryption does not matter. Spies may have to work harder on their targets but no communication, electronic or otherwise, is completely secure: it is just a question of how much effort the other side can put into getting hold of the message.

A much bigger worry for the spies is that the very vulnerabilities which make it easy for them to steal other people's secrets also make it hard for them to hold on to their own. In pre-computer days, intelligence agencies kept files on paper. Access was strictly controlled; making copies more so. That arrangement was cumbersome but made it possible to see exactly who had looked at a file, when and why. Looting an intelligence registry of its documents was all but impossible.

That has now changed. Computers are inherently leakier than cardboard files tied with ribbon and kept under lock and key. Any network connected to the internet is at risk of penetration. Even those that are "air-gapped"—kept physically separate—are vulnerable. A doctored mobile phone can secretly plant spyware on a target's computer and vice versa. Large quantities of data can be carried on a computer chip the size of a cufflink. In some quarters, for the most secret documents, manual typewriters and carbon paper are back in fashion.

This weakness was highlighted by Mr Snowden, who used his role as a lowly technician to extract a huge cache of documents from the NSA and other agencies. Only a fraction has been published (and, critics say, only a small number of those bear on his purported concerns about privacy and oversight). The NSA and allied agencies are still struggling to work out what was taken and assess the damage. Have the documents fallen into the hands of Russian and Chinese spooks, for example? British and American spies have already been moved from places where they may now be at risk; some have been given new identities.

Once more unto the breach

The Snowden breach—termed at the time the West's greatest intelligence disaster—is only one of many in recent years. Jeffrey Delisle, a Canadian naval officer arrested in 2012, was sentenced to 20 years imprisonment in 2013. For five years he had been passing Russia information from Stoneghost, a secret intelligence-sharing network for the "Five Eyes" countries (America, Australia, Britain, Canada and New Zealand). The Snowden files undoubtedly added details and gave ammunition to anti-Western propaganda outfits. But according to John Schindler, an American spy expert, the Delisle breach meant that Russian intelligence already "had it all".

Perhaps worse is the catastrophe at America's Office of Personnel Management (OPM). This low-profile agency handles security clearance for the millions of Americans who work for the federal government, and many of their spouses and children. Yet for more than a year, outsiders (probably Chinese spies, though American officials will not say so publicly) were running freely across its networks and databases, with the loss, by the latest tally, of information relating to 22m people.

This included the 127-page SF-86 security-clearance forms, on which candidates for sensitive jobs have to give an exhaustive account of their past, including foreign contacts. The OPM also lost another set of files: the so-called adjudication data, relating to sensitive personal details which had caused difficulties at work, such as extramarital affairs, sexually transmitted diseases and other health matters, as well as the results of polygraph tests. The OPM used laughably weak security and did not encrypt the data it held. The breach came when hackers stole the login and password of an employee working at a commercial contractor for the agency. The OPM's director has now resigned.

The OPM does not deal with current staff of the CIA and other agencies but that is no great comfort. The information enables Chinese (or other) counter-intelligence services to play "spot the spy". The core activity of a Western intelligence agency is to send its officers overseas as embassy officials. This is known as "official cover" and at some levels the

pretence is a matter of politeness. Titles such as "economics attaché", "first secretary (external)" and "counsellor (information)" give a semi-public signal of what the real job is.

Other identities are tightly concealed. Spies may work as lowly administrators or consular officials, performing routine tasks and seemingly of no interest to the hostile country's counter-intelligence services. But their real task is far more important: collecting clandestine communications from dead drops, watching out for signals from sources and so on. They may be in charge of meeting agents in inconspicuous places or supporting other spies working under deep cover, without the protection of a diplomatic job.

If 28 of the 30 purported officials at a diplomatic mission, say, are listed on the OPM's database, then it is a fair bet that two who are not must be undercover intelligence officers. It is also possible to work out which people have moved from the intelligence world to regular diplomatic and other government service. In short, if the OPM tells you who the real diplomats are, it is possible to identify the pretend ones. That helps a hostile foreign intelligence service work out what the spies have been up to. Past patterns of activity and contact, which seemed innocent at the time, can be re-examined to see if something else was afoot. That can lead to sources being caught, jailed or, in some countries, executed.

A further difficulty is that information about personal weaknesses is ripe for exploitation. Intelligence officers seeking to recruit a target work on four frailties, summarised in a CIA dictum as money, ideology, compromise and ego (MICE for short). A frank account of a target's financial woes, political views, sexual peccadillos and personality quirks makes that a lot easier.

Insiders reckon it will take decades for American intelligence to recover from the OPM breach. But rebuilding a human-intelligence service will be a lot harder in the digital age. Before the days of electronic databases and biometric checks, creating a new identity for a spy was easy. A well-used passport in a fake name, a wad of travellers' cheques and some visiting cards were enough.

Now creating a convincing fake identity is much more difficult. Anyone without years of credit-card, mobile-phone and utility bills is automatically pinpointed as a potential spy for the other side. These can be falsified, but it takes time and effort. Worse is biometric information. If you claim to be visiting Russia for the first time, but your facial bone structure, gait, retina scan or DNA shows you were there before under another name, you are in trouble. Spymasters cannot easily overcome these difficulties—using people with solid real-world identities who act as spies on the side is far harder than faking identities.

Technology has turned the spy world upside down. The benefits of successful espionage have never been greater. But so are the penalties for carelessness, both in public opprobrium and secret disaster.