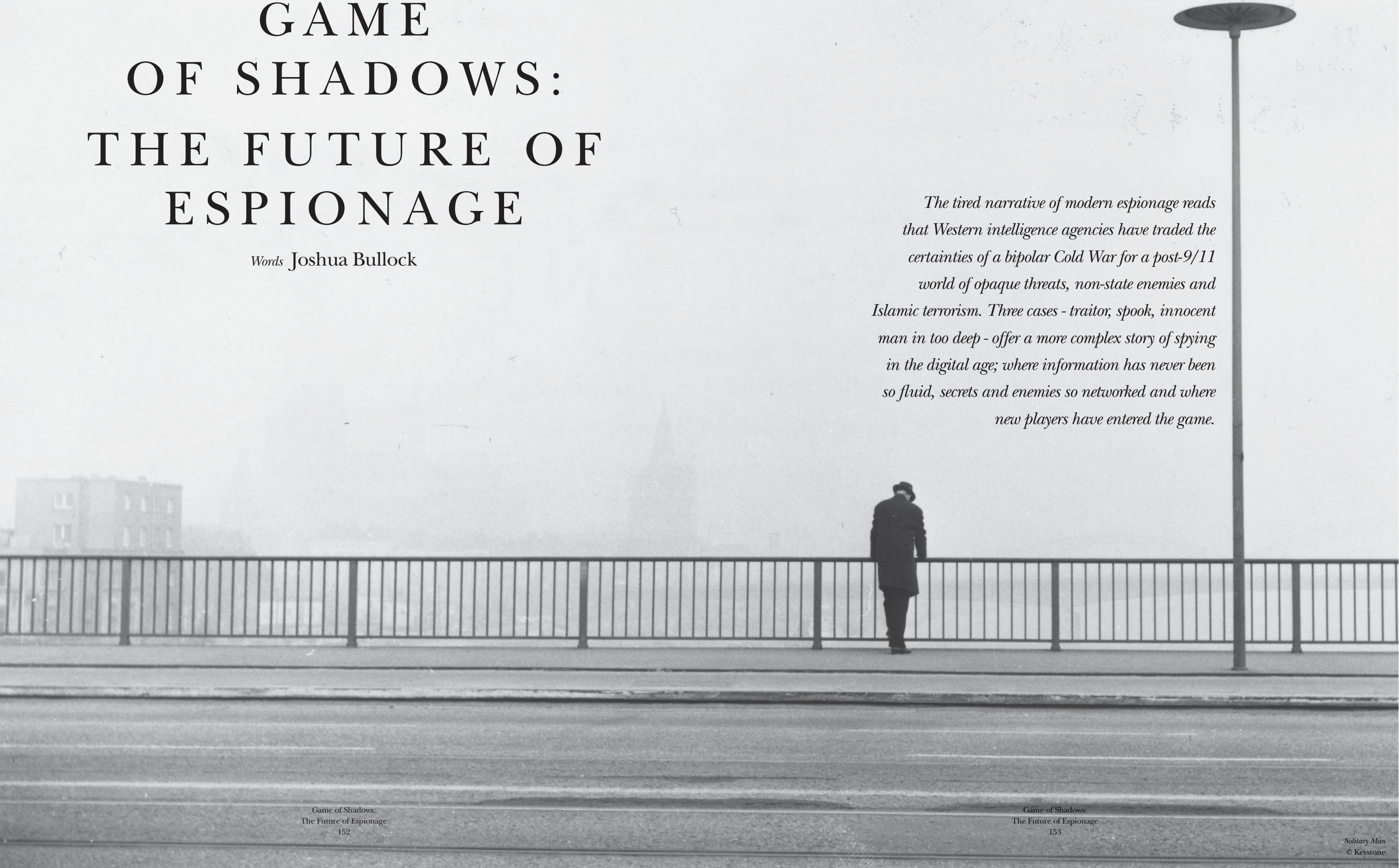
GAME OF SHADOWS: THE FUTURE OF ESPIONAGE

Words Joshua Bullock

The tired narrative of modern espionage reads that Western intelligence agencies have traded the certainties of a bipolar Cold War for a post-9/11 world of opaque threats, non-state enemies and Islamic terrorism. Three cases - traitor, spook, innocent man in too deep - offer a more complex story of spying in the digital age; where information has never been so fluid, secrets and enemies so networked and where new players have entered the game.



Solitary Man
© Keystone

In 2007, a Canadian naval officer walked into the Russian embassy in Ottawa and asked to speak to someone from Russian military intelligence. In a side room, Jeffrey Paul Delisle proposed almost laughably favourable terms. Until his arrest five years later, Delisle would smuggle secret documents out of a naval base on a USB stick relating to the Stone Ghost system that connected intelligence from the 'Five Eyes'- the United States, Britain, Australia, New Zealand and Canada - to give his Russian handlers. All he wanted was 3,000 Canadian dollars a month.

In 2012, an American electronics engineer Shane Todd was working at a Singaporean research institute called IME on a project in collaboration with Huawei, a Chinese telecoms giant. Perplexed by the nature of his research and its implications for his own country's security, he had contacted his family about his deep misgivings and was serving out his notice. He was found hanging in his apartment three days after his leaving dinner, surrounded by packing.

The police report stated that Todd had drilled holes into the bathroom wall for a pulley to kill himself. When his parents came to his apartment, they found no such holes. Nor did they find his laptops or mobile phone, which had been kept as evidence. Suspicious, they had the mortuary photograph their dead son and an independent pathologist concluded that the marks on his neck were consistent with garrotting. Dr Adelstein found it strange that the original Singaporean autopsy had also missed Todd's deeply bruised knuckles. The six-foot-one, 200-pound college wrestler had not met his tragic end quietly.

Despite these oddities, the Todd case might perhaps have suffered the same fate as that of Gareth Williams, the GCHQ (communications intelligence) spy found dead in a holdall in his London flat while on secondment to MI6 in 2010. The coroner had found the circumstances of Williams' death 'unnatural and likely to have been criminally mediated' but offered no inkling of motive. Murder without motive is the big story that sizzles then drowns in its own mystery. Williams' classified work and collaboration with American agencies led Foreign Secretary William Hague to sign an 'interest immunity certificate' for key evidence to be heard in private and withheld from the inquest. It seemed the Singaporean authorities and IME's lawyers had performed a similarly effective block on any deeper investigation into Shane Todd's death.

But as Todd's mother packed the last of her son's possessions in Singapore she noticed a small computer speaker and put it in the bag. Back in the U.S a few weeks later, his father realised the small speaker was actually a hard drive. It contained thousands of work files transferred during Todd's last day at IME. The work showed the details of the project he had been coordinating: designing an amplifier for civilian telecoms which had applications for radar and electronic warfare that major U.S defence contractors were also pursuing.

On 9/11, a group of mainly middle-class Saudis with little military training hijacked four planes and changed the course of world history. MI6 and the CIA's focus at the time was not fundamentalism, nor the industrial and military espionage of the Delisle and Todd cases, but rather international drug wars and countering the threats posed by WMD. If any reminders were needed as to the gravity of this new menace, the 2004 Madrid train bombings and 7/7 London attacks confirmed radical Islam as the clear and present danger in the eyes of Western security services.

Since 2005, the capacity of the Pakistani-Afghan-based rump of Al-Qaeda to conduct global Jihad has been steadily destroyed by well-briefed, surgical drone strikes and Special Forces raids. With Bin Laden and most of its original high and mid-level command gone, Al-Qaeda as an operating force has franchised into new ungoverned spaces: Syria, Somalia and most recently Mali and southern Algeria The shifting allegiances of these splinter groups and their relationship to other insurgencies are chaotic. Plans left by Malian Al-Qaeda fighters fleeing French troops this February outlined how Al-Qaeda in the Islamic Maghreb (AQIM) propose to parasitise the efforts of Tuareg rebel separatists, ethnic Arab militias and fellow Islamist groups like Ansar Dine – an organisation bound to Al-Qaeda in a similar way as the Afghani Taliban.

While a broad coalition of rebels and religious insurgents were seizing control of vast swathes of the Sahel between Sudan and Mauritania, Western resources were concentrated on Yemen and Somalia as the new hotbeds of Jihad. The hydra of extremism is global and the nature of the groups involved so parochial that intelligence services find themselves struggling to cope. There is no consensus on whether AQIM has plans to strike at foreign targets from this new operating base; there is only the sense of unease at facing another protracted insurgency akin to Iraq and Afghanistan.

What happens in Mali and other incubators of terror not only exercises foreign intelligence agencies like the CIA and MI6, but agencies charged with domestic security like the FBI and MI5. Former head of NYPD's counter-terrorism department Mitchell Silber: "There's now a much longer laundry list where a citizen can go to receive military training, some ideological confirmation, then come back to the West with a clean skin and look to carry out terror domestically." It was once a philosophical reach for American agencies to believe the U.S was facing homegrown terror. The Boston marathon bombings are another reminder to the contrary.

Whereas the UK and U.S were first focused on the threat from second and third-generation Pakistani and Middle Eastern Muslims, both countries have seen the profile of extremists change. In the U.S there have been a number of radical Hispanic converts as well as those of Balkan descent. MI5 have seen increasing radicalisation in Afro-Caribbean and Somali communities. The scale of the plots have become smaller, Silber says, with networks of a dozen plotters downsizing to a handful of individuals as the pressure exerted by surveillance and profiling bites.

In recent years, security chiefs have upgraded the threat posed by Iranian backed terrorism. An elite special operations arm of the Iranian Revolutionary Guards Corps called the Quds Force is an increasingly powerful voice in Iranian foreign policy. Quds were successful in supporting insurgents in Iraq and its commander Qassem Suleimani was known as the most powerful man in Baghdad when using proxies or his own agents against coalition soldiers. Iranian-American citizen Mansour Arbabsiar identified Quds as the group running him in his conspiracy to hire Mexican drug cartel assassins to kill the Saudi ambassador to Washington in 2011. The revelation that a high-ranking official would have legitimately sanctioned terrorist activity in the U.S capital has only boosted intelligence agencies' resolve in combatting Iranian efforts to secure a nuclear weapon and harass Western interests in the Middle East through proxies like Hezbollah.

Iran has long relied on espionage to counter their military shortcomings and paranoia over internal dissent sponsored by the U.S and Britain. Little known is the fact that Iran operates its European espionage activities from the Balkans, principally Bosnia, a stronghold established during their decades-long secret relationship with and sponsorship of the SDA, the dominant party among Bosnian Muslims. Iran has recently been implicated in the suicide bombing of Israelis in Bulgaria and had nine spies 'rolled up' in Turkey. Every victory for its spies is a fillip for a beleaguered regime under the yoke of international sanctions and internal ferment.

September 11 World Trade Center Attacks
Photo by Paul Turner
©Getty Images

Former Russian Agent Alexander Litvinenko is pictured at the Intensive Care Unit after being poisoned In London
Photo by Natasja Weitsz/Getty Images
@ Getty Images

Japan Coast Guard patrol the Senkaku Islands, East China Sea
© DigitalGlobe/Getty Images

Espionage as a projection of power has been dogma in Russian statecraft since 'The Great Game' its spies played against British agents in central Asia during the 19th Century. Mark Galleoti, an expert on Russian security affairs who runs the blog *In Moscow's Shadows*, says ex-KGB officer turned President Vladimir Putin sets the aggressive default tone. "Putin sees a world in which nothing is ever what people say. You've got protestors at home: infiltrate and isolate. Your economy is still nowhere near leading-edge technology: well, go and try and steal microelectronics through a Texan-based company." At time of writing, Russian sleeper cells in Germany and suburban America are standing trial. Jonathan Evans, outgoing Director General of MI5, has said Russian intelligence is as active in the UK as it was at the height of the Cold War.

By the time the Soviet Union collapsed, the KGB had developed an essentially nationalist, conservative and elitist identity. Galleoti explains how this permeates its modern successors: "They saw the outside world as a threat, as well as a great opportunity for them. That's carried through to the FSB, and also the SVR – essentially the old KGB's espionage arm, just with a new logo and new initials. They're based in the same building on the outskirts of Moscow."

We may never know, for example, the exact reasons for Alexander Litvinenko's death in 2006. What is clear is the former intelligence colonel was poisoned by radioactive polonium. The hit was a piece of theatre, sending out the message to 'Londongrad' émigré circles that dissent and collusion by defectors like Litvinenko would be repaid fully, as well as the West's support for dissidents and pro-democracy movements in Russia. While experts downplay Litvinenko's strategic importance, it reaffirmed Russian intelligence agencies' belief in their own creed and reoriented British intelligence back to the persistent Russian threat.

It seems likely that Putin's aggressive policies will be the high-water mark for the West's traditional foe. Russia's ailing economy means the resources poured into intelligence agencies are under increasing pressure. The FSB is analogous to a domestic security service like the FBI, while the SVR and the military GRU (who ran the Canadian traitor Delisle) are charged with foreign intelligence. The turf wars between these agencies are seismic. Russia's foreign ministry has long been exasperated by the influence they have on Putin's decision making. The GRU in particular has been very vocal in its support for Assad during the Syrian civil war, while the caution voiced by Russia's diplomats was ignored. With such competing interests behind the scenes, it is difficult to discern Putin's master plan.

The deep complicity between agencies like the GRU, organised crime and Russia's oligarchy means that much of the espionage Russia conducts is industrial in nature. Czech counter-intelligence reported that Russian intelligence assets were being deployed to help a Russian consortium win a nuclear power plant project. "It all speaks to this inter-penetration between politics, business, intelligence and, frankly, crime," explains Galeotti.

However, Russian industrial espionage pales in comparison to another. Espionage is Chinese economic policy turned outwards, as it pursues intellectual property it can steal and manufacture cheaply, particularly in communications and electronics, but also for military purposes. Perhaps Shaun Todd's death was part of this deadly game. James Mulvenon, specialist in the Chinese military and cyber warfare, talks about this revolution: "They have been able to take advantage of the fact that China is the world's information technology workshop, and they have been able to build a very sophisticated, multi-layered, encrypted architecture to support its military modernisation."

These technologies have been networked together in a "hybrid inventory of hardware" the Chinese use to pursue a geopolitical as well as industrial agenda against hi-tech enemies like the United States. Last autumn, *The New York Times* was so sophisticatedly breached by Chinese hackers it took weeks to spot, by which time information and passwords from the newspapers network had been compromised. The reason? China wanted to find the Deep Throat who had passed the paper information for a negative story on the fortunes amassed by the family of Wen Jiabao, the country's prime minister.

> Jonathan Evans, outgoing Director General of MI5, has said Russian intelligence is as active in the UK as it was at the height of the Cold War

The web is a new battleground and as the Internet increasingly hardwires institutions, it provides the conduit for subterfuge and all out assault. A Stuxnet computer virus destroyed centrifuges at Iran's Natanz uranium enrichment facility in 2010, while Iran has targeted energy companies in the Gulf through its cyber command. A complex cyber-espionage network called Red October, only discovered a few months ago, has been stealing data from networks across government agencies, research centres and energy companies the world over, with targets concentrated in Russia. It was Russian coded and Chinese operated.

Non-state actors are also causing intelligence chiefs sleepless nights. Cyber-criminals and anarchist 'hacktivists' - like Anonymous - embezzle and disrupt government sites and multinationals. MI5 reported that one London-based bank lost £800 million due to one cyber-assault. The UK's Security Minister says that cyber crime costs the country £27 billion a year through attacks on company systems, and industrial espionage ranks as one of the four main threats to national security alongside terrorism, natural disasters and major accidents. The European Cybercrime Centre began work this January, but in the absence of international consensus on how to regulate the web, a fiber optical melee of competing parties probe the digital defenses of businesses and governments.

As technologically far-reaching as American and British communications agencies are in electronic surveillance, the skillset of MI6 and CIA officers remains deeply rooted in analysis. A deep awareness, familiarity and knowledge of distinct cultures and how circumstances might be turned to nations' advantage are all reasons why spies need passports, not just laptops.

Spying is said to be the world's second oldest profession after prostitution and really the digital age has only diversified its skills. Perhaps it is only a matter of time before Jihad moves online, but cyber security and fundamentalism are only part of this game of shadows. The light some wish to shine on its murky trade will reveal disturbing pacts; for if we don't really know the stakes, we will never truly know how far spies will go to protect their masters' interests.