Finding the Russian Moles

by Michael Curtis

I've got my eyes on you so best beware where you roam. I've got my spies on you I'm checking all you do. Look you sir, inquire how and who, and where they keep, what company at what expense.

Espionage is an old story. Long ago Moses dispatched twelve spies. a group of Hebrew chieftains, to explore the land of Canaan as a future home for the Israelite people. They reported they had found a land flowing with milk and honey. On December 8, 2020 it was disclosed that individuals, almost certainly Russian, looking for the contemporary version of milk and honey, had hacked the U.S. security firm Fire Eye, only one of the many targets compromised in the cybersecurity industry. It soon became apparent that foreign hackers had attacked both governmental and unofficial organizations. A large-scale espionage campaign has breached the U.S. Treasury and Commerce Departments, and other government agencies. The campaign also affected non-governmental companies: Microsoft and customers were compromised, and emails had been stolen

from U.S. private sector companies. The victim of a highly sophisticated targeted attack, Orion Platform, the server of the network management system Solar Winds which produces software for the U.S. government and private companies, was breached.

Corruption and sabotage of network systems has now become an important concern. Cyber-attacks have been made on the White House, State Department, and the joint Chiefs of Staff. The intelligence agencies of Russia are all successor agencies to the KGB, the symbol of the Cold War, and are administratively independent of each other, and most report to the president of Russia. The SVR, the Russian Foreign Intelligence Service, is concerned with the collection of intelligence of foreign countries. The GRU, or GU, the main intelligence directorate, the primary intelligence agency of the Armed Forces, and reputedly the largest foreign intelligence agency, appeared responsible for hacking the Democratic National Convention in 2016. The FSB, Federal Security Service, designated successor to the KGB, appears to have moved beyond domestic security to operate internationally.

Espionage was not always like this. The traditional world of spies, not completely ended, was different, a world of personal searches, in an organizational context, to seek out information and hunt out traitors on behalf of presumed national security. The death of novelist John Le Carre on December 12, 1989 reminded us of the fictional presentation of the life of intelligence agencies and operatives: international intrigue, personal betrayal, flawed characters, deception, and subterfuge, emotional complexity, and ambivalence about being involved in intelligence activity or spying. These books of le Carre differ from what he called the "cultural pornography" of Ian Fleming's James Bond fantasies.

In le Carre's 1974 work, *Tinker, Tailor, Soldier, Spy*, the tale was focused on trapping a "mole," an active double agent for Britain and the KGB the former secret intelligence

service, a tale based on or alluding to Kim Philby, the real double agent. Involved is the struggle between le Carre's protagonist Smiley and the Russian spymaster Karla, a cunning struggle with a minimum of violence. The highly successful book of le Carre, *The Spy who Came in from the Cold*, the story of a disillusioned British agent involved in a fatal mission in East Berlin was a touching commentary on the tensions and duplicities in the Cold War era. The loyal and upright Smiley held there was nothing dishonorable in not being blown about by every little modern wind in that era where adherence to communism or democracy competed.

Recent deaths and arrest of spies have reminded us of the resemblance of that fiction to reality. One aspect is the formidable and aggressive Russian personal espionage, to some extent a continuation of Cold War espionage. A tantalizing example was the discovery and arrest in June 2010 of Anna Chapman, attractive, Russian born intelligence agent and model, part of the spy ring, the *Illegals*, network of Russian sleeper agents who posed as ordinary citizens but built contacts with political, economic, and academic figures to obtain information. But more important is the danger of cyber espionage and for the vital need for technology to provide computer protection against interference or illegal intercept of sensitive information by foreign countries.

The reality of espionage may be illustrated by two examples. One is the case of Victor Sheymov the Russian computer expert, a major in the KGB, who died on October 18, 2020 in Virginia, aged 73. He had been responsible for the cyphers and communications of the KBG, and helped prepare daily briefings for members of the Politburo. He defected to the U.S. in May 1980, because of the murder by the Soviet Union of a friend and fellow KGB agent for "dissident activity." He debriefed U.S. intelligence officials about the KGB's cryptological network. He told of the KGB plots, one was to kill Pope John Paul II; another was the assassination of the

Afghan in 1979. Sheymov knew that two members of the State Department spied for the KGB, and that there was at least one "mole" in the CIA. He also told the U.S. that the embassy in Moscow was completely bugged.

A more well -known double agent was George Blake, George Behar, who died on December 26, 2020 in Moscow, at age of 98. Blake was born on November 11, 1922 in the Netherlands to a Dutch mother and Egyptian father, a naturalized Briton. He came to England in January 1943 and joined the British navy. After the war he studied Russian at Cambridge and joined MI6. He was posted to Seoul, where he was captured by North Korean forces, and interned for three years, during which he, according to his own account, became a committed communist, allegedly because of his expressed horror of allied atrocities in the Korean war.

After release, Blake rejoined MI6, was sent to Berlin where he was supposed to recruit Soviet agents for British intelligence. But the opposite happened. Blake became a double agent, and passed British intelligence to his Russian handlers. He was finally exposed by a Polish defector.

Blake, a master of disguise with his typical English bowler hat and rolled umbrella, had MI6 posts in Vienna, Berlin, Milan, and Beirut, ran agents and betrayed every American and British agent he knew as well as his MI6 colleagues. A major accomplishment was reporting to the KGB Operation Gold, the building by the U.S. of a secret underground tunnel in divided Berlin running from the American sector into the Soviet zone, allowing western agents to tap Soviet phone lines and underground cables and listen to Russian communications. According to the CIA, Blake passed over 7,000 pages of classified British and American documents to the Soviet Union.

At his trial Blake was sentenced to 42 years prison, one year for every agent betrayed, though later he claimed he had

betrayed over 400. He was jailed in 1961, but astonishingly escaped from his prison Wormwood Scrubs in 1966. He was smuggled out of the country to East Berlin, and then to the Soviet Union where he spent the rest of his life. He became a lieutenant colonel in the KGB, was honored several times including in 2007 by President Vladimir Putin with the Order of Friendship, the highest Russian honor. Putin called him a professional of particular vitality and courage, a "legendary person who will be preserved forever in our hearts." Blake lived comfortably in a rent-free dacha thirty miles from Moscow. He was of enormous propaganda value for Russia.

What is significant is that Blake defected of his own accord, cooperating voluntarily with his adversary. This was unlike the defection of the well-known Cambridge double agents, Donald Maclean, Anthony Blunt, Guy Burgess, Kim Philby, and John Cairncross, who had been contacted by the KGB .

A Russian operative was General Igor Korobov, head of GRU military intelligence who officially died, aged 62, on November 21, 2018 after a "long and serious illness." He was accused by the U.S. in December 2016 of malicious cyber-enabled activities threatening the security of the U.S. Korobov was awarded Hero of the Russian Federation in 2017. His "illness" may have been the result of responsibility for some GRU failures. However the GRU had been active: it interfered in the 2016 U.S. election, it had hacked the computer of the international anti-doping agency, it had organized the coup in Montenegro in October 2016, it operated in eastern Ukraine, it snooped on the Dutch organization for the prohibition of chemical weapons in The Hague, organized cyberattacks on the UK and probably caused the destruction of Malaysian airlines flight 17 in July 2014.

But the GRU was humiliated in failing in the attempt to kill Sergei Skripal, and his daughter Yulia, in Salisbury. The former Russian military intelligence officer who became a double agent was called a traitor to his homeland and a

“scumbug” by Putin.

Uneasy lies the head of GRU operatives, who are prone to fatal accidents.

Korobov’s predecessor, Igor Sergun, died in 2016 in disputed circumstances, a deputy GRU chief was found dead on a Turkish beach, a major general fell out of a window, a senior official was run over by a car, the deputy head in 1992 was killed in a car accident. But the Russian global espionage campaign continues , made significant by the successful operations of the SVR and its APT 29 or Cozy Bear group. It is incumbent on the incoming U.S. Administration and the UK to identify and dispose of threats to national security. “I spy strangers” should be limited to the House of Commons.