**It's not just Laborers who are losing their jobs, Human Intelligence Collectors are losing their jobs.**

**What? That is unbelievable, incredible.**

Well, Friends, you have heard about all the cyber hacking that has been going on. Cyber hackers that attack our computer networks (Recall Solar Winds) that control our government agencies (including the Dept of Justice [FBI works here], the Dept of Energy, the Dept of Treasury, the Dept of State, Dept of Defense) infrastructure, or financial institutions, or airports, or large communications networks, are doing a lot more real, and theoretical, damage to us than 95% of the human spies have been able to do. I almost forgot they have shut down hundreds of our hospital computer systems too. They shut down the entire healthcare system in Norway. Patients will die if computer systems linked to operation rooms are disrupted.

Cyber hacking of America has cost us millions, and when successful at shutting down parts of our national energy distribution system and disrupting our national infrastructure, that is very serious, and even the KGB, now SVR, espionage operations, cannot harm us with such severity. Only the use of nuclear weapons is more threatening.

Actually, what really has changed is warfare, in peacetime, as well as in time of war. Cyber warfare are already being be used against governments in peacetime, as well as in combat. Our satellites have already been scanned by low power lasers, and I am certain that if conflict is initiated against any of our primary foes, the first wave of attacks will be against our satellites, which today, provide real time data for most of our military operations.

Our Air Force pilots and air missiles must have GPS to locate targets in foreign countries, our Army needs data for their missiles and also for locating enemy troops and weapons, and our Navy needs data for locating surface and underwater targets.

And what about our human intelligence collectors? There jobs are already complicated as face recognition has already complicated all our embassy/consulate personnel, once foreign governments can get a clear image of any person officially assigned to our foreign offices. They can conduct internet searches to learn a lot about all our internet activities - even what you last ordered at McDonalds. Anyone in the spy business who has debts, or disagreements with other people or organizations that has been disclosed on the internet, will find the information likely used against him/her.

=====================================================================================

**Source**: [***https://foreignpolicy.com/2019/04/27/the-spycraft-revolution-espionage-technology/***](https://foreignpolicy.com/2019/04/27/the-spycraft-revolution-espionage-technology/)

**Changes in technology, politics, and business are all transforming espionage. Intelligence agencies must adapt—or risk irrelevance.**

*By Edward Lucas*

Illustrations by Delcan & Company April 27, 2019



The world of espionage is facing tremendous technological, political, legal, social, and commercial changes. The winners will be those who break the old rules of the spy game and work out new ones. They will need to be nimble and collaborative and—paradoxically—to shed much of the secrecy that has cloaked their trade since its inception.

The **balance of power in the spy world is shifting**; **closed societies now have the edge over open ones. It has become harder for Western countries to spy on places such as China, Iran, and Russia and easier for those countries’ intelligence services to spy on the rest of the world.** **Technical prowess is also shifting**. Much like manned spaceflight, human-based intelligence is starting to look costly and anachronistic. Meanwhile, a gulf is growing between the cryptographic superpowers—the United States, United Kingdom, France, Israel, China, and Russia—and everyone else. **Technical expertise, rather than human sleuthing, will hold the key to future success.**

In another major change, the boundaries between public and private sector intelligence work are becoming increasingly blurred. Private contractors have become an essential part of the spy world. Today, intelligence officers regularly move into the private sector once they leave government. The old rule that you are “either in or out” has become passé. That shift has allowed some ex-spies to get extremely rich, but it is also eroding the mystique—and the integrity—of the dark arts practiced in the service of the state.

Finally, **intelligence agencies in democratic countries no longer enjoy the legitimacy bequeathed on them in the past or the glamor that rubbed off from Hollywood and spy fiction**. Public skepticism about the means and aims of a potentially money-grubbing, thuggish, and self-interested caste of spooks has grown. Spymasters increasingly have to justify what they do and accept unprecedented levels of legislative and judicial scrutiny.

The **biggest disruptive force is technological**. Traditional spycraft has always relied on deception based on identity. Spotting, developing, recruiting, running, and servicing intelligence sources involves concealing what you are doing. If you fail, your adversary may find out what you’re up to, endangering your source and totally undermining your efforts. Once an adversary learns that an intelligence operation is underway, he or she can use it to discover more clues or feed you false or tainted information.

Traditionally, spies depended on cover identities. Until a few years ago, a visiting Canadian in Moscow who claimed to be a graduate student in architecture could present a cover that would be difficult for Russian counterintelligence officers to crack. They could check her documents, grill her about her background, search her possessions, or follow her. They could even use a gifted individual with a photographic memory for faces to scour books full of pictures of known or suspected intelligence officers. But if none of those avenues produced any clues, all they could do was watch, wait, and see if the suspect made a mistake.

Not anymore. A cover identity that would have been almost bulletproof only 20 years ago can now be unraveled in a few minutes. For a start, **facial recognition software—mostly developed by Israeli companies and widely deployed in China and elsewhere—allows governments and law enforcement agencies to store and search vast numbers of faces**. **They can then cross-check such data with the slew of personal information that most people voluntarily and habitually upload online.**

**Counterintelligence officers start with the internet**. Has their target appeared in any photo anywhere? If so, was the context of that photo compatible with the target’s cover story? Then they use CCTV, gathered at home and from systems run by allies. If the Canadian architecture student does not appear in any social media linked to the Canadian university where she claims to have studied, her story starts to look shaky. It looks even worse if she can be seen on holiday in Hong Kong three years ago, socializing with U.S. officials based at the consulate there.

**A cover identity that would have been almost bulletproof only 20 years ago can now be unraveled in a few minutes.**

The **most crucial element of the technological storm engulfing intelligence agencies is the mobile phone**. This device not only records your communications once hacked—phone calls and messages received and sent—it **also acts as a tracking beacon.** It can easily be attacked to become even more intrusive. Given a minute of hands-on access, **an adversary can make sure that the microphone is turned permanently on and that the phone continues transmitting even when the owner believes it to be switched off.** The same malware can be installed by sending a text message.

One obvious solution would be to not carry a mobile phone or to use a “burner” device—a phone bought with cash and replaced frequently. But doing so creates an even bigger danger. In the case of the Canadian graduate student, having searched for her likeness online, a Russian counterintelligence investigator would then look at her phone data. If the investigator finds that she doesn’t have one, that’s highly suspicious. Only the very poor, the very young, and the very old don’t carry some kind of mobile device these days.

Of course, if the student does have a phone, but the number is new, that’s also suspicious. Most people seek to keep whatever phone number they first acquired even as they change devices. If the Russians then obtain her phone records (by hacking into her home provider’s database or bribing someone there to look them up), they can discover where she has been, who has called her, and whom she has called. Tracking her movements may reveal only a fleeting interest in Moscow’s architectural marvels—as well as other, more sinister interests. These might include stops on park benches, trips to obscure suburbs, or disappearances into the Moscow Metro during which the subject switched off her phone for hours.

**Investigators can also combine these two tactics with a third: financial information**. What is the student’s credit rating? What plastic cards does she carry? Does her purchasing history and behavior match her cover story? Every one of these questions is revealing if answered and devastating if not. There are, after all, very few people who travel abroad without a bank account or credit rating, with no social media history, and a prepaid burner phone—and those who do tend to have something to hide.

Intelligence agencies have several ways of addressing these technological problems. One is to throw money at them, spending time and effort creating a bank of impeccable “legends” (cover identities) for their intelligence officers. This technique starts with false names, documents, and addresses—the traditional stock in trade of the spy world—but with a digital twist. Today, spies can rely on a LinkedIn entry, a plain vanilla credit rating, or a dormant Facebook account, all with enough detail to be plausible but with too little distinctive material to make a serious check possible.

A second strategy is to use “cleanskins”—freshly recruited intelligence officers whose history reveals only their previous civilian lives. A third option is to treat identities as disposable—sending intelligence officers on one-off missions, knowing that afterward they will be burned forever. A fourth is to conduct espionage only in neutral or friendly environments: You still spy on the Russians or the Chinese but from London or Paris rather than Moscow or Beijing. None of these approaches is ideal. Either the risks and costs are high or the benefits are low—or both.

**The most crucial element of the technological storm engulfing intelligence agencies is the mobile phone.**

Meanwhile old staples of spycraft no longer work due to technological advances. Until recently, the dead-letter box was regarded as all but foolproof, an ideal location that both a source and a collection officer could plausibly visit—a bench in a cemetery for example. One party would leave behind some intelligence material, perhaps stored on a tiny memory card enclosed in chewing gum. The other party would then collect it. Even a team of experienced observers would struggle to see what was really going on.

Today such tactics rarely work. It is easy for Russian counterintelligence to track the movements of every mobile phone in Moscow, so if the Canadian is carrying her device, observers can match her movements with any location that looks like a potential site for a dead drop. They could then look at any other phone signal that pings in the same location in the same time window. If the visitor turns out to be a Russian government official, he or she will have some explaining to do.

Electronic communications have grown equally vulnerable. The more that intelligence agencies know about what normal behavior looks like, the more that anomalies and coincidences stand out: Why is the suspect using an internet cafe or a virtual private network? What websites is she visiting from her home computer and from her phone? Does she use encrypted messaging services? Has she developed a sudden interest in computer games (an easy way of sending messages to a source masquerading as another player)? What about her online shopping habits?

The same algorithmic techniques that digital security experts use to spot malware on networks and computers can easily be tweaked to highlight other unusual behavior—sometimes much more effectively than human analysts could. Together, **these techniques have severely constrained the ability of intelligence officers and their sources to operate safely and secretly.** The **cloak of anonymity is steadily shrinking**.

As Western spymasters seek to manage the challenges presented by new technology, they are facing far greater political and legal constraints than their adversaries. Indeed, authoritarian states have an advantage over liberal democracies.

Many Western societies are fiercely debating the issue of intelligence oversight—and that debate is healthy. But for all their flaws, there is a categorical difference between the way big Western agencies operate—under judicial, legislative, executive, and other constraints—and the means and methods of their counterparts in places such Russia or China. Getting access to mobile phone records in the West takes more than a mouse click. It typically requires a warrant, which must be sought through a bureaucratic process. **In Moscow and Beijing, it’s easy. Indeed, China’s national security law expressly requires every individual and corporation, state-run or not, to aid the intelligence services.**

The shift toward **electronic intelligence collection also creates new risks and political difficulties for all parties because it blurs the distinction between espionage work and warfare**. In the world of human intelligence, the difference between the intelligence services and armed forces was in theory clear-cut. An intelligence officer’s job was always to find things out, not to make things happen. Military personnel wear uniforms, and the laws of armed conflict govern their activities; when captured, they are meant to be taken prisoner. Spies and plainclothes saboteurs get shot.

**In the online world, attributing motive is far harder. An intrusion into another country’s sensitive computers and networks for the so-called innocent purpose of reconnaissance can easily be mistaken as an act of sabotage or at least preparation for it**. The potential for misunderstanding intent pushes cyberespionage practitioners into unfamiliar political and legal territory. Human intelligence agencies have developed norms, which to some extent substitute for the lack of legal regulation in what can never be a law-governed space. For example, **toward the end of the Cold War, both sides refrained from physical attacks on each other’s intelligence officers or their families. There are, to date, no similar arrangements in cyberspace.**

The same algorithmic techniques that digital security experts use to spot malware on networks and computers can easily be tweaked to highlight other unusual behavior—sometimes much more effectively than human analysts could.

As political scrutiny intensifies, Western intelligence agencies are operating in an unfamiliar and increasingly hostile environment. Public concerns about privacy have mushroomed because of the intrusive and careless behavior of tech giants. Trust in governments has fallen. Spies—in most democratic countries—cannot take public acceptance of their activities for granted. They must also assume that public opinion will continue to shift against them.

Spies today increasingly need to work with lawyers, both to counter adversaries’ reliance on lawfare—the use of the legal system to delegitimize an enemy or win a public relations victory—and to test the legality of their own operations. Even if national security exemptions apply to the details of sources, methods, and intelligence material provided to decision-makers, the legal environment is intrusive and constraining. A Western intelligence officer can no longer go on so-called fishing expeditions, trawling through emails and other private material in the hope of finding clues that will help steal secrets or catch spies. Instead, the breach of privacy has to be justified in advance and is also subject to retrospective review.

Privacy and human rights laws are placing more and more constraints on intelligence agencies’ activities, especially as they seek to gain new powers, such as compelling tech companies to help break into encrypted devices and communications. A 2016 ruling by the European Court of Justice, for example, risked making illegal all the bulk data collection conducted by Britain’s signals intelligence agency, GCHQ, on behalf of the U.S. National Security Agency. Intelligence agencies in the United States, Britain, and other Western countries now employ lawyers and public affairs specialists to monitor data protection and other laws.

As political scrutiny intensifies, Western intelligence agencies are operating in an unfamiliar and increasingly hostile environment.

Intelligence officials must also reckon with the fact that sanctioned illegality today may get them into trouble tomorrow. Extraordinary rendition of suspected terrorists, for example, has been the subject of intense legislative scrutiny in the United States. In 2012, Abdelhakim Belhaj, a Libyan émigré opposition figure, sued the British government for his kidnapping in Thailand in 2004 and forcible return to Libya, where he and his pregnant wife were tortured. In 2018, the British authorities paid the family compensation and apologized.

Such legal worries would have been unheard of during the Cold War, when no explicit legal framework governed spy activities. Now, due to freedom of information legislation in many countries, intelligence officers must reckon with the possibility that in 30 years’ time—when documents are declassified—they may be held accountable for decisions that seem entirely justifiable today but will be highly questionable by the standards of the future.

Indeed, what may seem trivial today will be shocking tomorrow because it clashes with accepted social norms. Take, for example, the use of dead babies’ birth certificates—a common way of creating a cover identity, first made public by Frederick Forsyth in his thriller *The Day of the Jackal*. When, between 2011 and 2013, it emerged that British undercover police officers were using this technique in order to infiltrate radical political groups, the public erupted in outrage, leading to a series of high-profile government inquiries and expensive legal settlements.

The technique in question had involved a secretive unit called the Special Demonstration Squad, which trawled birth and death records to find details of children who had died in infancy, secured their birth certificates, and then obtained driving licenses and other documents so that they could masquerade as protesters and sympathizers, gaining the trust of the groups—sometimes by having intimate relationships with members for years. But such tactics were only useful when dealing with targets with no serious counterintelligence capabilities. The danger of finding a death certificate matching the supposedly “live” individual has increased as a result of digitized public records. Instead, intelligence agencies today do something even more offensive to modern social mores: They look for people who are never going to apply for passports or create any digital traces of their own.

A favorite category is people born with profound disabilities, who spend their lives in the care of others. A disabled man who has no bank account or mobile phone and requires round-the-clock care for his most basic and intimate physical needs is going to be invisible to the outside world. But he has a birth certificate, which can be used to build an identity for someone else’s undercover life. This practice raises profound ethical questions in an era when most people feel that those with disabilities have inalienable human rights. What may have been acceptable 20 years ago may seem outrageous and career-killing in 20 years’ time.

The booming world of private intelligence companies is watching these techniques and their practitioners with a greedy eye. Indeed, the intelligence profession is increasingly overlapping with the corporate world. The world of spies used to be cloistered. People who joined it never spoke about it and often served until retirement. Penalties for disclosure could include the loss of a pension or even prosecution.

That has changed. A stint at the CIA or MI6 has become a paragraph on a resume, not a career. Britain and the United States have caught up with Israel, where the private sector has long prized a spell in a senior position in intelligence or defense. In London and Washington, such work is increasingly a launchpad for an interesting career in corporate intelligence or other advisory work.

Government intelligence agencies have stopped battling the commercialization of espionage; instead, they embrace it—a practice exemplified by the Israeli company NSO Group, which, according to a *New York Times* investigation in March, is one of several firms that broker the sale of former government hackers’ expertise to countries such as Saudi Arabia. Security clearances in the United States and United Kingdom used to lapse on retirement. Now, retired intelligence officers are, in many countries, encouraged to maintain them. Retirees may be hired as contractors, or they can make job offers to people still inside the service.

Intelligence officials must also reckon with the fact that sanctioned illegality today may get them into trouble tomorrow.

And when the tricks of the trade—bugging, impersonation, hacking—are illegal, they can simply be outsourced to a suitably unscrupulous subcontractor. The food chain in the private spy world is highly respectable at the top, with former spymasters offering exquisitely priced and presented inside information about the way the world works.

Further down the ladder, things are different; if you want to find out where your rival’s corporate jet has been flying, someone with access to the air traffic control database will provide the answer in exchange for a fat envelope. The theft of electronic data is effectively untraceable: There is no need to download the data; you can just photograph the computer screen with a mobile phone. Or the data can be obtained by impersonation—infiltrating the target organization undercover as a temporary secretary, security guard, or cleaner.

Meanwhile, public tolerance is waning as knowledge, trade-craft, and contacts gained at taxpayer expense are used for self-enrichment in retirement. The conflicts of interest and other pitfalls are obvious. Many of the techniques used by government spy agencies are intrinsically illegal (including bribery, burglary, bullying, and blackmail). Such lawbreaking raises the question of what happens if a client hires a private company that is also the target of a government investigation. Must the private company sacrifice its profits? Who makes it do so?

As the cost of conducting espionage operations—in money, time, and effort—has shrunk, spying has become less esoteric. These days it is an integral part of business, finance, sports, and family litigation over divorce and child custody. Indeed, modern life encourages people and institutions of all kinds to adopt the thinking and practices of the spy world. Are you worried about your date? Then you will find open-source information establishing whether he or she has a criminal record, bad credit, unfortunate habits involving drug use, or unusual sexual preferences. The same goes for prospective hires.

**Anyone responsible for a company’s cybersecurity now has to think like a counterintelligence officer**.

Anyone responsible for a company’s cybersecurity now has to think like a counterintelligence officer. To protect a firm’s sensitive information, he or she must identify the most gullible and careless members of the organization and fire them or give them better training. The long-standing practice of opposition research became an everyday phrase during the U.S. presidential election in 2016. Republicans determined to undermine Donald Trump hired a firm founded by Christopher Steele, a former top MI6 Russia hand, to dig for dirt. When Trump won the Republican nomination, the research project continued—but with the firm allegedly being paid by Democratic candidate Hillary Clinton’s campaign. Steele’s research involved contacts with the FBI, which some critics say crossed the public-private and serving-retirement boundaries.

The rise of commercially available spying technology has led to some savings for governments in money, risk, and time**. Investigative outfits such as Bellingcat, using open-source information, commercial databases, and material hacked or leaked by sympathetic allies, have produced startling scoops and exposes, including identifying the three would-be assassins of Sergei Skripal, a former Russian military intelligence officer who had retired to the quiet English town of Salisbury.**

Competition raises standards, in spycraft as in other fields. Intelligence agencies need to work with other actors outside the spy world, both in order to find out what is going on and in order to influence it. **Spies and intelligence chiefs need to be media-savvy, countering and mounting information operations. In the old days, spymasters told spies that any contact whatsoever with a journalist was a sackable offense.**

That dividing line is now thin and full of holes. **Intelligence officers find plenty to talk about with journalists. They can discuss the credibility of open sources and the difficulties of operating in hostile environments. Intelligence officers involved in “active measures”—making things happen rather than just finding out about them—can find it useful to brief journalists, either highlighting solid facts and logic that help their case or on occasion inventing or twisting source material in order to produce new coverage with the requisite slant or spin**.

Given this changing landscape**, spies also need to be at home in the worlds of business and finance.** Unraveling the webs of offshore companies that lie behind Iran’s evasion of sanctions, Russian oligarchs’ influence operations, or China’s exploitation of its ethnic diaspora has become a formidable task.

A few years ago, I coordinated the defense in a libel suit brought by a Russian tycoon against the Economist, for which I had worked as the Moscow bureau chief. An article by a colleague had implied that this man’s riches were due to his personal and political connections with Vladimir Putin. We were able to spend hundreds of thousands of dollars on a detailed, forensic investigation of a segment of the energy market that we believed our target was manipulating. After the case was over, a spy chief from another Western country told me that finding a few hundred thousand dollars in cash to bribe a North Korean would be no problem. Spending the same amount on statisticians and lawyers would be deemed unacceptable, however. Intelligence budgets are for spying, not finding things out through legitimate means.

That’s because spy agencies will not be able to maintain the levels of operational secrecy that they have come to regard as routine if they enlist the help of lawyers, journalists, accountants, business executives, and academics. If you hire a law firm, what happens if its computers are hacked or its staff suborned? The wider you spread the zone of secrecy, the more fragile it becomes.

Yet the biggest impediment to successful spying today is not leaks but excessive classification. The security clearance industry, particularly in the United States, operates with agonizing slowness, hampering the recruitment of useful people (such as the multilingual children of immigrants) and letting through liabilities (such as Edward Snowden).

If you hire a law firm, what happens if its computers are hacked or its staff suborned? The wider you spread the zone of secrecy, the more fragile it becomes.

Information in most countries is also ludicrously overclassified, at too high a level and for too long a period of time. Overclassification and excessive secrecy do not protect countries from their adversaries. Such methods only protect bureaucrats from scrutiny. Intelligence agencies use the supposed need to protect sensitive sources and methods to justify their concealment of blunders or activities that deserve public scrutiny. This excessive secrecy makes spy services timid, introverted, risk-averse, and calcified by procedure. Taxpayers end up paying ever greater bills for ever less impressive results. Meanwhile, the enemies of Western democracies, untroubled by such procedures, steal secrets and meddle in U.S. and European politics with abandon.

In the coming years, the bigger danger could be the opposite one: The intelligence services of democratic countries may become too flexible and too deeply involved in the institutions and procedures of a free society. The temptation to do so will be particularly strong in countries facing the full blast of hostile influence operations, such as Australia (which faces a Chinese threat) or Ukraine (which faces a Russian one). Intelligence-led criminal justice sanctions and regulatory sanctions—arrests, asset freezes, deportations, banning media outlets, and so forth—that should be the exception could become the rule.

Most of us don’t want to live in a country where the leadership spends all its time reading intelligence briefs, where the intelligence and security agencies are at the heart of public life and political decision-making. I once lived in a country like that: Putin’s Russia. Western democracies need the intelligence services to defend open societies against Putinism—but not at the price of self-Putinization.

***Edward Lucas is the international editor for the* Economist**