The world of information is changing at light speed. Covert operations run by the top-notch intelligence agencies are uncovered with cameras in hotels and shopping malls. Low-budget terrorists run operations using free imagery from Google Earth. An army of amateur sleuths exposes secret rendition flights from out-of-the-way military airports on several continents. Top-secret State Department cables, once meant for the eyes of a few, are leaked en masse through a phalanx of servers around the world.[68]

In this environment, how can anybody run an intelligence agency?

9

THINKING ABOUT INTELLIGENCE

THE FUNDAMENTAL PURPOSE of intelligence services is to prevent surprise, especially strategic or grand-scale surprise. "No More Pearl Harbors" was the cry after 1941. And two years after the Second World War ended we created the CIA and the Defense Department. The NSA followed in 1952. "No More 9/11s" was the cry after the Twin Towers fell. And again we adjusted our budgets and made organizational changes. Compared with preventing surprise, everything else is secondary. But preventing surprise is difficult. It requires an understanding of an adversary's intentions as well as its capabilities. Capabilities invariably have physical manifestations. You can count numbers of tanks and missile silos. You can monitor missile tests to observe accuracy and reliability. But intentions are more elusive—and may be detectable only when it's too late to do anything about them. Is a country modernizing its navy to protect its own coast, or does it have expeditionary intentions? Against whom? These questions are difficult to answer.

Preventing surprise also requires that we not be taken unawares by the emerging technologies that erode boundaries, accelerate change,

and confound our ability to control them. As we have seen over and over again, these technologies are creating previously unimaginable transparency—voluntary and involuntary, good, bad, and indifferent—in all walks of life: personal, commercial, governmental, and military. These developments profoundly affect intelligence organizations' capabilities and manner of operating. In order to understand how these developments affect them, however, we must first make clear what intelligence is.

THE CORE FUNCTION of intelligence is stealing secrets.

Most descriptions of intelligence work break it into two lines of business. Stealing secrets is called "collection"—though, as we will see, intelligence services also collect plenty of information that isn't secret. Collecting is done through human spies, whose principal business is persuading foreigners to commit treason; through electronic penetrations of foreign information networks; or through sophisticated imagery and sensors designed not only to photograph but also to sense radiation, chemicals, and other invisible emanations from installations that a foreign government or transnational terrorist group wants to keep secret—like a clandestine nuclear facility, or a factory for making nerve gas. The same technology lets us monitor the radiation resulting from a nuclear accident in a friendly country. Even people who are uncomfortable with the entire intelligence enterprise want us to know about such things. Other departments of government also collect information, but not secretly. The Department of Agriculture collects information about world grain markets, for example. The State Department collects information about foreign governments, but while diplomatic cables may be classified, diplomats' collection methods are open and aboveboard. In contrast, the core competence of intelligence agencies is stealing information that cannot be gathered openly.

The second principal line of work for the intelligence business is

analysis, which is collating classified and unclassified information and making sense of it. These two activities—collection and analysis—are supported by scientific research and other secondary functions, but the collection/analysis dichotomy is basic and is reflected in the organization of our foreign intelligence agencies. In the CIA, for example, the Directorate of Intelligence (analysis) and the National Clandestine Service (spies) are supported by the Directorate of Science and Technology and Directorate of Support. The NSA's organization is somewhat different because that agency also has a defensive function to protect classified networks,[1] but within the NSA's offensive operation, the collection/analysis dichotomy also holds true. Still, bifurcating intelligence this way can't give us a full sense of the business, because it omits a great deal. For example, counterintelligence, which in my view is a core part of the intelligence enterprise, isn't essentially about stealing secrets. It's about defeating the efforts of foreign intelligence services to penetrate the U.S. government and American companies, either by disrupting their efforts or misleading them.[2] The FBI's recent roll up of ten Russian illegals was a counterintelligence operation. So was the CIA's reported booby-trapping of the computer chips that the Soviets secretly diverted to use in the trans-Siberian pipeline, which then blew up. In counterintelligence's defensive mission, which is protecting secrets, transparency is a nightmare, because it makes secrets hard to keep. In its offensive mission, which is disrupting foreign services, transparency is an advantage.

The collection/analysis dichotomy also omits covert operations, which intelligence agencies in all countries have carried out for centuries. Strictly speaking, a covert operation—that is, an operation that may occur in the public eye but whose true author is disguised[3]—is not about gathering or analyzing information. It aims instead to do something openly that nobody wants to admit having done. The Dubai assassination was a covert human operation that achieved its objective but left lots of clues about who did it. Designing and spreading the

Stuxnet worm that corrupted Iran's nuclear command-and-control system was a covert electronic operation. We don't know yet—and we may never know—how successful it was or who did it. Governments assign this kind of covert operation to their intelligence services because the operations require extraordinary access to secret information, whether it's the travel plans of Mahmoud al-Mabhouh or the design and specifications of an adversary's networks and plant equipment. These operations also require the ability to conduct secret business across continents. In the United States, most of the criticism directed at the CIA has been triggered by its covert operations and not by its intelligence-gathering activities.

During wartime, intelligence services find themselves drawn into yet another kind of covert operation. At the start of the current war in Afghanistan, for instance, a small number of highly skilled CIA officers performed extraordinary feats in dislodging the Taliban from power, and since then, CIA officers have run many paramilitary operations in that theater of war. Although these operations require stealth and intelligence support, they are not fundamentally an intelligence function. We assign them to the CIA chiefly because no other organization in the U.S. government is nearly as agile. The military can and does run covert operations too, but compared to the CIA, the military is far more bureaucratic.

The collection/analysis dichotomy also leaves out the intelligence community's huge and growing responsibility for spreading information swiftly throughout the federal government, to state and local governments, and sometimes to private industry. The agencies still think of this as ancillary, if not opposed, to their core lines of business, but it is actually now at the heart of their work. It requires the ability to sort and collate vast troves of data, assess their importance, and send them where they need to go—but not to everybody at the same classification level or in the same level of detail. This work eats up hundreds of millions of dollars annually in equipment and time, and as the WikiLeaks

document dumps have demonstrated, unless it's done right it creates pervasive vulnerabilities, by making classified information available to the wrong people. Frankly, this kind of wholesale dissemination effort is anathema to the ethos of intelligence professionals—and not because of bureaucratic jealousy. It's anathema to them because any information that's distributed en masse, whether or not it is classified, simply isn't secret anymore. To understand this, suppose that our man in wherever is the only person who knows certain secret information about a foreign government's intentions. Suppose further that the risk of losing this secret through treachery, negligence, leaking, or any other reason is x. As soon as our man tells his colleague or boss, the risk doubles to 2x. But when our man puts that information into a network to which ten thousand people have access—many of whom are less well trained to keep secrets than he is, or who have never met the source of the information and don't lose sleep (as he does) about his source's fate if he's uncovered—then the risk of losing the secret increases by a factor of more than ten thousand. At that point, the information may still be sensitive, but we're kidding ourselves if we call it secret. Secrets have a half-life; they degrade over time. The more people who know them, the faster they degrade.

Finally, the collection/analysis dichotomy obscures the morphing of analysis into two distinct lines of work. I'll call the first line analysis proper. It consists of the sifting and winnowing of lots of information and figuring out what it means. The second line is classified journalism, or turning conclusions into finished products for the president and other high officials. Journalism is not a pejorative label. The ability to take a complex subject and express it in clear, concise prose is a rare and valuable skill, but it's a different skill from doing analysis proper. Operationally, the two skills have always been closely related, but they are different, and the pressures on them are different, too.

With this background, let's return to the question at the end of the last chapter: How can you run an intelligence agency in a world where secrets, if you can keep them at all, don't stay secret for long?

A casino
Las Vegas, Nevada
10:12 P.M.

The heavyset man in the safari vest had been at the blackjack tables three nights running and his winning streak was impressive. Certainly the sharp-eyed watchers in the video surveillance booth upstairs were impressed. They were also suspicious. The man moved from table to table, every night playing with several dealers. He was a professional, they could see that, and won more often than he lost. That kind of skill costs the casino money and will earn you their attention. So up in the booth one of the security staff began to log this gambler's playing time, rerunning videos from the previous nights and calculating his winnings at each table. This showed her what she had missed in real time: The man gravitated to one dealer more than the others, and he won more consistently with that dealer—for three nights running. Who was he?

According to his California driver's license, which he had presented to get credit for his gambling, he was Edward McNeil Partland, and he lived in a rented apartment in Torrance but picked up his mail at a PO box—nothing too unusual about that. He had an account with the Los Angeles Department of Water and Power and one with T-Mobile for cell-phone service. He didn't use Twitter, but he did have a Facebook account. Partland listed his occupation as security consultant, freelance. He looked legit. But if he was a pro, why did none of the Las Vegas casinos have any record of his previous gambling? He also had a tattoo on his right forearm of the 101st Airborne Division, with its screaming-eagle logo. The security crew upstairs began to dig deeper, checking commercial databases that ordinary people don't buy access to.

Yes, Mr. Partland had an address in Torrance, but he had been at that address for only three months. Yes, he had an account with L.A. Water and Power—also for about three months. Before that, nothing. He had a California driver's license, but why did a nationwide check disclose a driving record that went back less than a year, when he supposedly moved to California? A check of a multistate vehicle insurance database turned up nothing older than twelve

months. How could an army veteran who appeared to be about forty-five years old not have a long history of auto insurance? So casino security dug deeper. Why, they wondered, did Mr. Partland have a tattoo of the 101st Airborne on his arm but no record of military service? And why couldn't they find any trace of him in any of the 101st Division's veterans' groups? They looked at his Facebook account, but there was little on it—and no "friends" from the army. Nothing in Mr. Partland's story could be proved false, but the whole story was just too thin, and the security team could smell it. Real people leave lots of trails. Their identities are thick. Meanwhile, "Mr. Partland's" luck held out. He was a hundred thousand dollars ahead of the house. And then, after the fourth night, he stopped coming.

The security staff turned their attention to their dealer. Let's call her Angela Raney. (She's my invention, just like Partland.) Casinos don't hire dealers without investigating them up one side and down the other, and Ms. Raney was no exception. She lived right in Las Vegas, sharing a bungalow with a longtime boyfriend named Ben Taylor. The casino knew about Taylor; if you work for them, they know a lot about you. So it didn't take long to pull his record of military service and discover that he had served during the first Iraq War in the 101st Airborne. A little more digging found that before moving to Vegas, he had lived in Torrance and had used a PO box address—the same PO box used by Partland. Suddenly, using only mouse clicks, a scheme to rip off the casino was coming apart: "Ed Partland's" cover was blown. A crooked dealer, the dealer's lover, and the lover's army buddy were about to get acquainted with the district attorney.

THIS PIECE OF FICTION has nothing and everything to do with intelligence tradecraft: nothing to do with it because it involves a crime scheme to defraud a casino rather than spies and state secrets; yet everything to do with it, because Partland's cover problem is fundamentally the same as the problem of creating deep and effective cover for covert government operatives. Creating effective cover was never simple, but

it has now become much more difficult and expensive. Whether or not the cover involves an alias, the tools for prying it open are cheap and readily available. In either case the agent must have a detailed history, and that history must stand up to an intense level of electronic scrutiny available to any novice private eye, who will have access to a rich trove of information going back to the agent's school days.

Several conclusions follow. Serious cover will be used more sparingly than in the past, and fewer risks will be taken with it. This point bears emphasis: Clandestine services will become more risk averse. Training a good agent takes years. If sloppy cover exposes that agent, she is burned forever, and a big investment goes down the drain. The penetrability of cover will affect clandestine services around the world, and the more wired the country, the sooner the effect will be felt. This is not to say that technology is doing away with spies. Spies have been around since before Joshua sent his agents into Canaan, and they are not going out of style. Nor is transparency going to bleed treachery and deceit out of the range of human character traits. Indeed, it is more likely to put a premium on those traits. But the training of agents and the strategies for deploying them are already changing, and the risk that these agents will be stripped of their cover is going up. The Dubai affair will reverberate through the world's intelligence services for a long time.[4]

TO ENTER THE watch floor, you walk up a slightly elevated ramp—the wires that connect all that computer equipment have to go somewhere; they're under the floor—then through a door with a cipher lock. All employees have top-secret clearances, but they can't come in here without a reason. You pass through a comfortable but Spartan outer office, then stop to let your eyes adjust. The lights are low. And it feels chilly, especially in summer: In this environment people adapt to the needs of the computers, not the other way around, and computers must be cooled. The ops center is a kind of miniature amphitheatre,

with several levels of elevated seating, like a university classroom. Analysts beaver away on each level, some in military uniform, some not, each with his or her workstation and screens, each working a different issue. Behind them, in glassed-in cubicles, sit the watch supervisors. The front wall is plastered from waist height to ceiling with a bank of big video screens. Information is flowing in from all over the globe, sometimes just strings of numbers that only a specially trained analyst can understand, but there are also video feeds and interactive maps that bring together data from across the entire intelligence community and the military—exactly the sort of high-tech information sharing you had hoped was afoot among government intelligence agencies. It's amazing—even though you have no idea what most of it means. A couple of screens are familiar, however: one's tuned to CNN, another to Fox News.

Now the man in the booth is standing up and pointing. Suddenly the image on one of the screens disappears and another collection of pixels pops up. It's a cartoonish but near real time map with symbols of military units—blue and red, us and them—together with live radio chatter (which you can't hear because you're not wearing headphones). It looks cool, but it isn't. It's a schematic image of a firefight in Ghazni, a town in eastern Afghanistan where a NATO patrol is being ambushed from three sides, and blood is flowing. You're watching an extraordinary display of technological prowess that would have been impossible to pull off even a few years ago. But soon the supervisor sits down; there's nothing he can do. Air support is being called in, but not from here. Military command and control in the war theater takes care of that.

Ten minutes later Wolf Blitzer on CNN breaks off his chatter and cuts to a live video feed from Ghazni. A CNN reporter and cameraman are embedded with the NATO unit, and they're taking fire, but the camera's rolling, and they're pushing out live video and commentary against the barking rattle of machine-gun fire. This, too, is a display of technological prowess that would have been impossible a

few years ago. CNN's video actually contains less information than the government's integrated tactical sources, but it's an astoundingly good source nevertheless—which is why some watch-floor screens are tuned to commercial networks. In fact, you don't have to be on a multimillion-dollar, top-secret watch floor to see this video. You could be home drinking beer and watching it on TV.

FOR INTELLIGENCE PURPOSES, knowing about that firefight ten minutes before it hit CNN made no practical difference. No one in his right mind would say that our intelligence agencies, let alone the military, should rely on cable news or any other commercial source for tactical intelligence—at least, not now. But in the future questions like these will grow more pressing, particularly when it comes to political and social intelligence as opposed to tactical military intelligence, when minutes matter and commanders must be able to count on the capability to produce the intelligence every time. Whether a government should invest in a particular capability will depend on two factors: Will it be there when we need it? And can we do anything useful with the information if we're getting it only minutes before it hits the commercial source? Depending on the answers to these questions, the government may disinvest in some of the resources on that watch floor.

I have smart friends in the business who insist that this kind of disinvestment will never happen, that the agencies will never rely on commercial sources this way. But I fear that my friends aren't thinking far enough ahead—or looking far enough backward. We already rely to a significant extent on commercial satellite imagery (which is extremely good) to supplement the government's own satellite imagery (which is better). Thirty years ago few people in the Defense Department or the intelligence business would have believed that possible. The convergence of the technologies available to the most powerful

governments with the technologies available in your living room will not stop. And it will certainly drive public investment decisions.

Convergence is driving intelligence in another dimension, too. When an intelligence agency can get information that nobody else can get, it gains an advantage. Economists call this "information asymmetry." Everyone else calls it keeping the other guy in the dark. Either way, it's an advantage you want, whether you're the president of the United States, a currency trader, or a washing-machine salesman. Markets achieve optimum results when everybody has the same information, but an individual in a market thrives on having better information than everyone else. When traders get such information, they keep it secret. When governments get it, they classify it. When others can get it as readily as the government, classifying it is pointless, even silly.[5]

Yet most of what is worth knowing in the world is not classified, and technological convergence will make this axiom truer than ever. Everybody knows a lot, and secrets have a very short shelf life. In 1815, a difference in bond prices between the Paris and London markets might persist for days, even weeks. Today traders arbitrage differences between markets around the world in tiny fractions of a second. In 1842, news of the disastrous British retreat from Kabul during the first Afghan war took weeks to reach London. Today we have electronically connected journalists embedded with combat units in Afghanistan. The advantage that intelligence services once held in gaining access to information has shrunk.

The secrets our intelligence agencies steal, and the sources and methods that enable that theft, are valuable—but they usually have less to do with high policy than most people think. Unlike certain diplomatic cables, most of the information we secretly collect does not relate directly to the strategic intentions of adverse foreign governments, such as a planned surprise attack. When we collect information about adversaries' intentions, it's often tactical—a likely position in a negotiation, for example, or the fact that a secret missile test is about to occur, or that the test fizzled. These are real secrets. They are

important to know, and our agencies are extremely good at ferreting them out. But these are not strategic intelligence victories.

Strategic failures, on the other hand, don't generally result from a lack of capability but from a lack of imagination. Before December 7, 1941, for example, the U.S. Navy was certain that the waters of Pearl Harbor were too shallow for torpedoes. They couldn't conceive of scientists in another country—an Asian country, no less—solving this very problem, which indeed the Japanese had done. Of course there were other reasons for that disaster. Complex events always have many causes, but failure of imagination caused the greatest intelligence lapse possible—the failure to prevent surprise. North Korea's invasion of the south in June 1950 was another strategic surprise. U.S. intelligence was caught flat-footed—and so was the national security staff in the White House. In 1950, the CIA was less than three years old and the NSA didn't exist. Still, the problem wasn't a lack of an ability to spot massed troop movements. Intelligence agencies attend to the priorities their political masters downtown give them, and gathering intelligence on North Korea simply wasn't a priority. The entire national security establishment was focused on the possibility of war with the Soviet Union in Europe, not Asia. Inability to think beyond one's deeply held assumptions is not a peculiarly American problem, however. Before the Yom Kippur War of 2003, Israeli intelligence had plenty of information about the massing of Egyptian troops on the west side of the Suez Canal. They just couldn't imagine that the Egyptians would dare cross it. And so they suffered grievous casualties in the Sinai and on the Golan Heights before they could turn the military situation completely around.

Lack of imagination was a factor in the 9/11 disaster, too. Nobody took seriously the idea that al-Qaeda operatives would try to fly fully loaded airliners into buildings in the United States—in spite of intelligence suggesting al-Qaeda's interest in that tactic, and in spite of the fact that the FBI knew Zacarias Moussaoui was interested in flying large airliners but didn't care about taking off or landing. Lack of imagination can't be fixed by supplying more information.

Intelligence agencies have little if any competitive advantage over private companies in analytical talent and imagination, and their advantage in global reach is diminishing. As Columbia University's Richard Betts has pointed out, "No one can match analysts from the CIA, DIA, or NSA for estimating what Al Qaeda might do in the next month. But what is their advantage over Middle East experts in think tanks or universities for estimating worldwide trends in radical Islamist movements over the next decade?"[6] The leaders of the American intelligence community and Defense Department know this. That's why they spend many millions of dollars every year consulting with experts in universities and the private sector. This official scouring of unofficial sources of expertise is yet another example of the progressive breakdown of the once-clear boundary between the roles of the public and private sectors.

This isn't simply a matter of privatization. When the postal service hires a farmer's wife to deliver mail in rural areas, or the army hires a contractor to wash dishes instead of using privates on KP, those are limited forms of privatization. When the postal service contracts intercity mail carriage to a trucking company, or the State Department decides to use an armed security service rather than the marines for embassy security, those are deeper forms of privatization. However, all of them involve greater or lesser degrees of control over the activities of the contractors, who are working for the government. But when an intelligence agency elects to supplement its satellite coverage with commercial overhead imagery, and it alters its investment plans accordingly, something more profound is occurring. This isn't privatization in the usual sense. Rather, the government becomes just another large buyer of goods or services that it used to provide internally. It relies on the private sector (whose camera may be on a satellite launched by a French or Chinese rocket) to perform a function once thought integral to one of its agencies and exclusively within the power of the government. Low-budget terrorists already rely on Google Earth for intelligence. In a word, this is an example of unbundling intelligence into

component parts, some of which can be done as well—or well enough, or better—by the private sector.

To understand the future of the private sector's role in intelligence, we don't need a crystal ball. We can just as well look backward as forward, because we are experiencing a return to a historical norm. In 1815, for example, news of the French disaster at Waterloo first reached London not in the saddlebags of the duke of Wellington's courier, but in those of the courier paid by Nathan Rothschild.[7] The British government had no advantage in international communications over a wealthy banker. Both could hire couriers, establish a beaconing system using bonfires on hilltops, and hire fast boats to cross the English Channel. The electric telegraph did nothing to change that essential public/private equality. Private parties had access to the telegraph, and any man with pliers, a knife, and the ability to climb a pole could cut the line to disrupt someone else's ability to communicate. Not until the twentieth century, when cryptography and cryptanalysis required large sums of money and the secret collaboration of topflight mathematicians, did a few governments acquire qualitative advantages over everyone else in secret communications. The Second World War and most of the cold war cemented rich governments' near monopoly on intelligence, because only such governments could operate through war zones and on the other side of the Iron Curtain. With the advent of high-altitude surveillance aircraft, followed by surveillance satellites, this monopoly began to seem both natural and inevitable. It might even have seemed "inherently governmental."[8] Only the United States and the Soviet Union could compete systematically on this level. Even in the human spy trade, technology played a role in making the spy game seem like a government-only business. Spy cameras hidden in tie clips, low-voltage recording devices hidden in cigarette lighters, exploding cigars—these were the stuff of state security services (and Hollywood). You can now buy most of this stuff on the Internet, and the tiny camera in your cell phone is as good as any spy camera ever hidden in a tie clip. Our intelligence services remain far ahead of the commercial sector in

clandestine technical capabilities, but as the world has accelerated, this advantage is shrinking.

In the nineteenth century security services were largely a private-sector affair. The most famous detective agency in the United States, if not the first, was the Pinkerton National Detective Agency, organized in Chicago in 1850 by a Scottish immigrant, Allan Pinkerton. Pinkerton's business in the early days consisted chiefly of providing security to railroads and their cargo. His contract to protect the Illinois Central was drafted in 1855 by the railroad's counsel, Abraham Lincoln. After Lincoln's election in 1860, security for the president-elect was not provided by either the military or the Secret Service, which did not yet exist.[9] It was provided by Pinkerton and his men. In May 1861, Major General George McClellan asked Pinkerton to create a Secret Service for his army operations in Ohio—essentially a private version of what became the U.S. Army Intelligence and Security Command. Pinkerton also ran counterintelligence operations in Washington, D.C., during the Civil War.[10] The Justice Department was not created until 1870. A year later Congress appropriated fifty thousand dollars to the department for "the detection and prosecution of those guilty of violating federal law." The department found the sum insufficient, however, and engaged the Pinkerton Agency to handle the job.[11] Government lawyers today would regard all these functions to be inherently governmental.

Already by the late 1960s the sums spent by private firms for protection had reached half the amount of public expenditures at all levels for police, counsel, and criminal courts, and at least one social scientist saw the "apparent muddling of the public and private police function."[12] Although some private police may do some investigative work, they mostly perform security functions, which should not be surprising, since the police function has historically had more to do with keeping order than solving crimes after they occur.[13] Universities, hospitals, banks, owners of large apartment buildings, and nightclubs all employ private police or off-duty municipal police who act in a private

capacity. So do some wealthy residential enclaves. Starting in 1970 when the District of Columbia Court of Appeals held a landlord liable to a tenant who was criminally assaulted in the common area of his residence,[14] court decisions have provided an incentive for this kind of private policing. By 1970, a study of private police concluded there was "no clear-cut basis for distinguishing public and private police as to service performed."[15]

In today's world protecting the president certainly seems about as inherently governmental as you can get, but President Lincoln didn't think so. He and his advisers trusted Allan Pinkerton to gather intelligence and provide physical security; they didn't have a good alternative. Today, however, federal law (at least on its face) requires agencies to decide whether a particular activity *must* be performed by government employees based on whether that activity is *in its nature* inherently governmental. Indeed, under current federal law there is no middle ground: The categories commercial and inherently governmental are mutually exclusive, and every agency is required to parse all its activities into one of these two bins. This rigid, mutually exclusive duality is practically and logically untenable,[16] but it remains the touchstone of federal law in this area. The civil servants who write regulations like this are intelligent and experienced, but they are less interested in logic than in crafting rules they can administer to control the sprawling world of government contracts. They do the best they can with the legal tools they inherited from a world in which boundaries seemed stable. This tool is rapidly approaching the end of its useful life, however. Not many decades ago most Americans would have thought that delivering the mail was an inherently governmental function, and the history of public mail service supported that view. Then came Federal Express, UPS, and DHL (which began as a private company and was later acquired by the German post office). Military logistics and support also used to seem inherently governmental, but nowadays private contractors deliver ammunition, prepare food, and provide heavily armed security service. Whether any of these developments is good or

bad is important but beside the point. Good and bad don't correspond with governmental or commercial. As the world around us changes our assessment of what the government can do best, and of what the government alone should be permitted to do, changes too.

Apart from the deliberate, forceful taking of life, liberty, or property from its own citizens, or binding the government by contract, it is difficult to see what actions are inherently governmental. This isn't to say that the government should outsource everything it is permitted to outsource, but simply that the centralization of power in industrial societies that reached its peak in the mid-twentieth century is ending, and the intelligence business will not remain unaffected.

IN A VIDEO commercial IBM's Jeff Jonas is standing by an intersection with cars whizzing by, and he asks, "If all you had was a snapshot of the traffic five minutes ago, how would you know when to cross the road?" You wouldn't. In the future everybody will know a lot, and as Jonas rightly says, successful organizations will be those that can make use of what they know as soon as they know it.[17] Speed, not secrecy, will be the coin of the realm.

This is why the collection/analysis dichotomy in the intelligence community has begun to collapse, though the collapse is lamentably not yet reflected in the way our agencies are organized. Under the old model, operatives were kept rigidly apart from analysts. They were (and still are) organized in separate directorates with distinct cultures and usually collaborated poorly. Both were heavily white, male, and Ivy League, but the operatives were the supersecret guys who did the cool stuff and got to break rules. The analysts formed a mandarinate of well-educated specialists in history, politics, economics, and international relations. They decided *what things meant*, and for the most part they would tell you *what things meant* only when they were good and ready to tell you, if in their opinion you needed to know. They delivered their wisdom in the form of a finished product. These products represented

"Intelligence" (spelled with a capital "I"), which was based chiefly on secret sources, and which they distinguished from less well-informed thinking—or thinking not based on stolen secrets.

Sketching the traits of this community can easily and unfairly degenerate into caricature, however, so I emphasize that intelligence analysts as a whole were and are a highly capable cadre of civil servants who do credit to their agencies. But the isolation and privilege of a top-secret world lead to the sins of pride and self-satisfaction, which lead to error. Besides, working on a model that required a finished product meant their output was too slow. The relentless acceleration of nearly all aspects of life following the end of the cold war has undermined this model, and it has been strained nearly to the breaking point by a decade of terrorism and war in South Central Asia. We no longer face the rigid, slow-footed, technologically clumsy adversary of the cold war. Our adversaries are numerous, and they are deft, swift, and technologically skillful. Whether the threat was to the London Underground, a NATO facility in Germany, or a company of soldiers on patrol in Helmand Province, the demand for intelligence was becoming heavily tactical and ever more urgent. The agencies' customers needed information in real time—not after the mandarins had chewed the intellectual cud and uncapped their fountain pens. These customers were also becoming increasingly military. This is hardly a surprise during wartime, but because the pace of war has increased along with everything else, it means that intelligence has been pulled into tactical targeting decisions to a degree previously unheard of. In World War II, in order to be certain of taking out one target, 1,500 B-17s had to drop 9,000 250-pound bombs, which were accurate only within a radius of about 3,300 feet. In the Vietnam War, thirty F-4 fighter-bombers had to drop 176 bombs to destroy one target. During the first Persian Gulf War, in 1991, a single F-117 could reliably destroy two targets with two 500-pound bombs—if the weather was clear. During the current Iraq War, a single B-2 can reliably destroy sixteen targets with 16 bombs, in any weather.[18]

This startling qualitative improvement has required more than merely a huge leap forward in weapons technology. It also required a breathtaking leap forward in intelligence capability, *and* the integration of intelligence with weaponry. The army may have a tactical missile that it can guide into an apartment window from twenty miles away to take out a terrorist commander, but the officer who fires it had better know exactly which window to send it through. Precision is useless without intelligence, and the intelligence must be available to the soldier or pilot with his finger on the trigger. Getting this right is not done with carefully polished intelligence products of the sort that were the norm during the cold war. Now it is done by putting fresh tactical intelligence, sometimes with little evaluation, into the hands of battlefield commanders. This requires actually embedding intelligence officers in combat units, and it demands that collection, analysis, and operations be highly integrated.

We have become very good at this integration at the tactical level—that is, on the ground in battle. But regrettably this fluid integration of skills and information is not reflected in the organization of our agencies or even in the prevailing model of how the intelligence business is supposed to work. The orthodox account of intelligence workflow goes like this:

1. Elected officials determine intelligence priorities (e.g., to understand the nuclear weapons program of a certain country).
2. Intelligence officials, through an interagency process, translate these priorities into requirements (e.g., determine how long it will take that country to develop a nuclear weapon).
3. Collectors gather information to fulfill requirements.
4. Analysts figure out what it all means.
5. Congress decides how to invest in future capabilities based on executive branch recommendations—in an unrelated process.

In practice, collectors do not gather information to fulfill requirements, which are far too general to provide operational guidance. In the language of the trade, they collect against *targets*, which are specific people, facilities, or systems that may yield information from which the answers to broad requirements can be inferred. Leaving analysts out of the process of selecting targets—which is what the orthodox workflow model does—is unwise, because analysts can enrich the conversation by explaining what information they would need in order to address the requirements. Analysts know the analytic gaps better than anybody else. On the other hand, collectors understand potential access points better than anybody else. Operating in collaboration, these two groups make better decisions about target selection than either can make in isolation. Together they can also advise on both near- and long-term investment decisions: If only we had the means to find out such and such, we could target this requirement more effectively. In the next budget cycle, let's propose to invest in that capability. Creating organizational arrangements in which the analysts and collectors systematically collaborate would improve each of them.

The intelligence community has begun to attack several specific problems in just this way, but these efforts are the exception to the governing organizational model, not the rule. We must change the model. Organizing the business around problems rather than around functions (like collection) or capabilities (like satellites) would improve it greatly. Our budgets should be driven accordingly, but they are not. Instead, we budget around capabilities. Major change will not occur without congressional approval, however, because Congress controls the budget, and capabilities have constituents, particularly the corporate variety that manufacture and support hugely expensive systems. Corporate constituents make campaign contributions; problems don't. Just as there is a military-industrial complex that President Eisenhower warned about, so there is an industrial-intelligence complex with deep interests in the status quo. Both these alliances have a third axis, and that axis is rooted in the Congress of the United States.

At its extreme the pressure to make intelligence immediately available at the tactical level can push analysts completely out of the picture. This is dangerous but not surprising. Insofar as analysis involves the packaging of information for customers, it's a specialized form of journalism, and all forms of journalistic media are being hollowed out by a flood of information that does not flow through the traditional organs of large newspapers, wire services, or television networks. This is a form of disintermediation, or taking the middleman out of the transaction between the consumer and the source of goods, services, or information. And it is happening in intelligence analysis for the same reasons that it has happened everywhere else.

If you want information, you don't have to buy a newspaper; you can get it online. If you want shoes or tires or computers or clothes, you can buy them all online. As for books and music, networks have not only disintermediated the stores that sell them, they're disintermediating the books and CDs themselves. Physical books and CDs are just devices for delivering prepackaged, portable information. Now you can pick and choose the bits and bytes you want, in portions of text, stories, songs, and videos, ignore what you don't want, and download them directly. The ability to move information this way has enormous advantages for intelligence, just as it has in other transactions, but it also carries disadvantages. Much of the information that now circulates so freely is garbage. Intermediaries—that is, editors, publishers, retail stores, and intelligence analysts—performed a filtering function that we must now do ourselves or pay someone to do. They told us what was reliable, desirable, and important.

In intelligence work, the analog to garbage in cyberspace is incorrect or misleading intelligence. More than once I've seen military officers in the field and political ax grinders in Washington draw half-baked conclusions from unassessed intelligence—an isolated intelligence report, for example, that led inexorably to a certain conclusion, but only if you didn't know that the source was unreliable, or that the report was contradicted by three other reports, or that the language didn't mean

what it seemed to mean when read in isolation. That's why we prefer analysts to vet raw information before we disseminate it. Analysts are experts, and experts really do know things. Experience matters. But managing the tension between the need for immediate information and the value of vetted, analyzed information is difficult. This is another reason why the boundaries between collection, analysis, and customers are loosening. Not long ago these boundaries were sacrosanct, but they represent industrial-age organization, and they are too rigid to work anymore.

Intelligence analysis has also come to resemble journalism in its feedback loop—the effect of the observer on the thing observed. And here it's essential to distinguish between what I have called analysis proper, or the evaluation of evidence and drawing of conclusions, and the packaging of those conclusions for policy makers, which is a form of journalism. The media not only reflect what goes on in the world, they also affect world affairs by changing perceptions, and by giving publicity to people and events that would otherwise die in obscurity. Election polls affect voter behavior, for example. Reports of bizarre behavior generate copycat bizarre behavior. Reports of terrorist actions generate copycat terrorist actions. The visually spectacular effects of some events generate reactions that are often out of proportion to their real effects, to the point where the distinction between perception and reality vanishes.

Similarly, leaked reports that the intelligence establishment has reached a conclusion will affect diplomacy and the public positions of the president and cabinet. Only a few years ago it was almost unheard of for the conclusions reached in National Intelligence Estimates (our most definitive form of finished product) to be reported in the press or in an open congressional hearing. Now conclusions are leaked with appalling regularity by policy makers and their civil service underlings who disagree with them and seek political advantage by politicizing the analysis. This occurred notoriously in the case of the 2007 estimate

stating that the Iranians had at least temporarily stopped developing a nuclear warhead, but that was hardly the first such occurrence.[19]

Leaking has become so common that it has affected the language, manner of presentation, and sequencing of conclusions in some estimates. For a time it also led to pressure to preempt leakers by making at least a summary of the conclusions public. So much for the ability of intelligence agencies to render top-secret analysis! This is transparency run amok. It is also feedback with a vengeance, and the feedback operates in both directions. Of course the analysis may affect the behavior of the policy makers who sought it in the first place, but that is intentional. In the other direction, however, the anticipated reaction of the media, legislators, public, and foreign governments to whom it is likely to be leaked affects the analysis. This is an unintentional and perverse effect of transparency, and we must learn to live with it.

All administrations have been willing to leak information for political advantage. The recent Bush administration was no exception, and the Obama administration has carried indiscretion to new heights—for no apparent advantage at all—even as it has prosecuted leakers with commendable vigor. In his 2010 book *Obama's Wars*, Bob Woodward describes a meeting in Chicago on December 9, 2008, between president-elect Obama, then-CIA director Michael Hayden, and then-DNI Mike McConnell. Hayden and McConnell were briefing the president-elect on the series of worldwide clandestine counterterrorist operations that required the president's personal approval. These are among the most closely held secrets in government. Yet Woodward refers to specific operations in specific countries and to the "tens of millions" the CIA was paying to Jordan's General Intelligence Department and other foreign services.[20] Where did Woodward get this information? No one I know thinks it came from Hayden, McConnell, or the president. Every shrewd person I know thinks it came from one or more of the advisers close to Obama with whom he would normally have shared it. But whoever leaked the information got nothing for it.

The leaks came from people who were simply indifferent—or hostile—to the government's ability or right to keep any information secret.

This kind of indifference has long affected the press and the public. Here, for example, is a sentence of a kind we read so often that we no longer notice its puzzling, even oxymoronic use of the word secret:

> Earlier this summer, the United States resumed secret drone flights performing military surveillance in the tribal areas to provide Pakistani commanders with a wide array of videos and other information on militants, according to American officials.[21]

There is no meaningful sense in which these operations are secret. They may be classified, they may be unacknowledged, but they aren't secret, as this reference to them in the *New York Times* proves. As this indifference to secrecy spreads, it is bound to affect relations between the intelligence and political communities in both the executive and legislative branches. There is again less trust, and where there is less trust there will be less candor. Gresham's law when applied to information will do its work: Bad information will drive out the good. The dross will be shared, and the gold nuggets taken out of circulation and held privately. This would be dangerous in any government, and in a democracy, poisonous. But it is happening.

Candor in official documents is difficult enough in the best of circumstances. In the most recent (2009) edition of the unclassified *Quadrennial Intelligence Community Review*, which is prepared by experts from a variety of intelligence agencies, the authors' task was to forecast America's position in the world in the year 2025. This is a difficult undertaking, to be sure, but psychological ambivalence and political sensitivity muddled the overarching conclusion, as illustrated by this sentence: "Although U.S. influence will decline, America and its ideals will retain global preeminence." Since preeminence is largely measured by influence, it is difficult to know what, if anything, this sentence means, and in any case it is contradicted several pages later,

where we read of "the declining military, economic, and technological preeminence of the U.S."[22] Possibly these inconsistencies resulted entirely from a breakdown in the usually rigorous editing process, but I don't think so. This kind of language results from public officials' reluctance to speak plainly about the relative decline of American influence for fear of being accused of not believing in the unlimited greatness of the United States. For results that are both imaginative and candid, projects like the *Quadrennial Review* should be handled by the open-source arm of the intelligence community and contracted out to three or four trusted private firms *in several different countries*.[23]

As early as 1992, the chairmen of the House and Senate intelligence committees began pushing for more use of open-source information, to no effect.[24] Four years later the Aspin-Brown Commission proposed that the collection and analysis of open-source information be a "top priority." Again, the idea went nowhere. Secret organizations have a built-in bias in favor of classified over unclassified information. Any bias is suspect, but in the tsunami of data created by the information revolution, this particular bias is a serious handicap.

Only in the aftermath of the attack on the Twin Towers did the idea of an emphasis on open-source information gain traction. In July 2004 the 9/11 Commission recommended the creation of an open-source intelligence agency.[25] And in March 2005 the WMD Commission recommended creating open-source cadres within both the CIA and the Office of the DNI.[26] Later that year, spurred by these reports, the new DNI, John Negroponte, and the CIA director at the time, Porter Goss, announced the creation of an Open Source Center, to be housed at the CIA.[27] But the wizards of Langley immediately put their stamp on the new center by ensuring that nobody could work in it who didn't have a top-secret clearance, thus closing the lid on really imaginative change. As a result, the best work on open-source information now takes place in private companies that contract with agencies to collect and analyze open-source information. This is actually an excellent arrangement, but the fact that it took years to achieve it is an accurate

indication of the acute resistance to change at big agencies like the CIA, the NSA, and the FBI.

Operating in a classified environment is a serious constraint—more serious than most people in that environment realize. It is a drag on how they communicate, whom they communicate with, and how they do business, and it disconnects them from the realities of the commercial world. Yet people who have never operated outside that environment cannot imagine doing business any other way. Young recruits entering the business are frequently turned off by our agencies' stodgy business practices, conflict aversion, and mind-numbing PowerPoint presentations. Dispelling this atmosphere would dramatically improve the intelligence business.[28]

At the same time, clandestine and covert operations are best undertaken by people who have trained for years in the dark-side atmosphere, and who will never fully trust people who do not share that background. This ethos is a matter of survival. Efforts to open up that operational environment are misguided and doomed to fail. So as we examine the present and future state of our intelligence agencies, we see an increasingly irreconcilable disparity between open-source and covert. The former cannot operate effectively in a top-secret mind-set, and the latter can't work without it. Secrecy and openness simply cannot get along in the same organization, and this is why the bundle of activities that constitute the intelligence business will inevitably begin to come apart over the next decade. This unbundling is overdue. If we are going to protect what must be kept secret, we must separate it from what is not secret.

A salutary effect of the separation would be to stop funding secret organizations that produce mere journalism. During the French presidential election of 2007, while I was the national counterintelligence executive, I did an experiment. Several times a week I read official reports of the contest between Nicolas Sarkozy, the center-right candidate who eventually won, and Ségolène Royale, the Socialist Party candidate. I also read accounts of the campaign in the *New York Times*, the *Washington Post*, and the Paris daily *Le Monde*. There was no

information in the official reports that could not be found in the *Times* and the *Post*, and none of these American sources was as detailed or interesting as what I could read in *Le Monde*. It was obvious that the official "intelligence" was written from unclassified sources, yet the official reports were classified "confidential." Why? *Because that's what we think. The sources may be unclassified,* I was told, *but our conclusions are classified.* In some cases this reasoning makes sense, but in this case the only "conclusions" were a rehash of publicly available polling data.

Another excuse for producing classified intelligence of this ilk is that policy makers want it. Like people in the intelligence business, policy makers in the White House and on Capitol Hill privilege the classified over the unclassified, believing that the top-secret stuff must be the real juice. Besides, access to classified information is a sign of power. Playing to this mystique is craven. When intelligence officials have nothing secret to report, it's their job to say so. The State Department can do the rest. Rehashing unclassified information about foreign affairs is a long mile from the core business of intelligence, which is stealing secrets.

IN A WORLD where secrets, if you can keep them at all, don't stay secret for long, the best way to run an intelligence agency is to focus tightly on the parts of the business that are really secret and separate them from the rest. You spend more money on open-source collection and analysis, and let them happen in controlled but unclassified space. You beef up counterintelligence. And you pay much more attention to the electronic handling and dissemination of information—which is the subject of the next chapter.

Transparency exposes the government's secrets in the same way that it exposes corporate secrets and invades personal privacy—and for the same reasons of ready electronic access. Electronic information is liquid, and liquid leaks. Apart from the technology, our culture also disposes us toward transparency and inures us to the exposure of

information that not long ago would have been carefully and successfully hidden. Advertisements for adult diapers or remedies for sexual dysfunction, and an eager willingness to parade one's marital failures on television, are enabled by a profound cultural change. Whether you call this change an increase in candor or a decrease in shame—or both—is irrelevant. The change cannot seriously be doubted, and it makes us disinclined to keep secrets, or even to take secrecy seriously as a useful value in human affairs. The analog at the national level is a presidential adviser willing to retail information about covert operations to the media, and the everyday occurrence of headlines about "secret" military operations in Iraq or Pakistan. To the extent we are in a postprivacy world, we are also in a postsecrecy world.

The terms *postprivacy* and *postsecrecy* are useful if they help us understand a social sea change and the parallel between privacy and secrecy, but they are exaggerations. What we can say without exaggeration is that organizational secrecy and personal privacy are both under relentless assault. Secrets are harder and harder to keep, and matters that are successfully kept secret are likely to remain so for shorter periods of time, assuming they're of any interest to anybody. This is true whether the secrets are personal (like your medical records) or organizational (like CIA rendition flights) or both (like the allegedly fudged expense records involving a personal relationship that reportedly cost the chairman of Hewlett-Packard his job). If you're unknown and say nothing controversial, our beehive culture will leave you in peace. If you do or say something controversial, or simply become well-known, you risk being swarmed. People will think twice before saying what they think. This is a nasty prospect created by cybervigilantes.

It would be absurd, however, to think that there will be no more secrets.[29] As long as people feel any vestige of shame or can suffer from guilt, they will want to keep secrets. As long as secrets convey power over others, people will keep secrets. Blackmail is merely the extreme case of such power. The mere fact that someone knows that you know his secrets conditions his behavior. "Write nothing down, throw

nothing away"[30] would be the motto of any organization small enough, and secret enough, to get away with it. In business affairs people will keep secrets as long as information conveys commercial advantage. As long as governments want to engage in activities they wish to disavow, as long as governments do not trust one another and fear for their own security, they will go to great lengths to keep secrets and discover what the others are up to—and to try to hide how they go about it.

I have former colleagues who spend most of their working lives dealing chiefly in the most sensitive information imaginable, with lives hanging in the balance. For them the discussion of openness is bewildering. But their world is opening up nevertheless. If we are serious about keeping secret the work such people do, our intelligence agencies should jettison everything that is not demonstrably done better on the dark side. Their kind of work does not thrive in an open environment. More than half a century ago an adviser to President Kennedy, McGeorge Bundy, observed a tendency to protect all information as if it were top secret. "The moment we start guarding our toothbrushes and our diamond rings with equal zeal," he said, "we usually lose fewer toothbrushes but more diamond rings."[31] Today we still classify far too much information, but that persistent tendency has obscured a far more pervasive development: We have gone to the opposite extreme, and as the WikiLeaks fiasco demonstrates, we now treat diamond rings like toothbrushes.

Transparency and network anarchy have disoriented us. Now it's time to regain our balance and manage this predicament.