Foreign Affairs

Sunday, March 1, 2015
Disrupting the Intelligence Community
Jane Harman

JANE HARMAN is Director, President, and CEO of the Woodrow Wilson International Center for Scholars. She was a nine-term U.S. Representative from California and, from 2002 to 2006, the ranking Democrat on the U.S. House Intelligence Committee.

America's Spy Agencies Need an Upgrade

Some 40 years have passed since the Church Committee's sweeping investigation of U.S. intelligence practices, fresh on the heels of the Watergate scandal. And ten years have gone by since the last major reorganization of the country's spy agencies, enacted in the wake of 9/11. Both efforts led to a host of reforms—among them, the creation of the Senate and House Intelligence Committees, the passage of the Foreign Intelligence Surveillance Act (FISA), and the adoption of the Intelligence Reform and Terrorism Prevention Act, which I helped shepherd through Congress.

New challenges have prompted talk of change once again. The U.S. government's recently acknowledged drone program, the contractor Edward Snowden's leaks about the National Security Agency's surveillance activities, and the Senate Intelligence Committee's recent report on CIA detention and interrogation practices have fanned public anxieties about government overreach. Surprise developments, meanwhile, have blindsided U.S. officials. The disintegration of Syria, the Boston Marathon bombing, the precipitous rise of the Islamic State of Iraq and al-Sham (ISIS), the systematic hacking of U.S. computer networks—in one way or another, all caught Washington flat-footed. Last November, *The Washington Post* reported that CIA Director John Brennan was weighing a wholesale reorganization of the agency, one that would combine operational and analytic divisions into "hybrid units" dedicated to specific regions and threats. The paper's sources described the plans as "among the most ambitious in CIA history."

Yet rearranging the deck chairs will not be enough to prepare the intelligence community for the challenges that lie ahead. Instead, Washington must venture beyond the conventional wisdom and reckon with an alternative vision of the future. Imagine this: Ten years from now, the CIA's primary mission will be covert action, an arena in which the agency can make a uniquely valuable contribution to national security. The NSA, for its part, will move away from collecting personal data, since private-sector firms have the resources to do the same task. And traditional espionage—the use of spies to gather human intelligence—will become less valuable than open-source intelligence, especially information gleaned from social media. In each case, change will come rapidly. So rather than adapting slowly and haltingly, it may well be time to accept reality and steer into the skid.

LICENSE TO DRONE

Since President George W. Bush declared a “war on terror” in 2001, the CIA has gotten extremely good at killing terrorists. The agency’s talent for targeted killings has made more than a few people uneasy, however, both inside and outside Langley. As Elliot Ackerman, a former CIA paramilitary officer, wrote in The New Yorker last November, “The discomfort of my colleagues, where it existed, didn’t stem from [targeted killing] itself. . . . The discomfort existed because it felt like we were doing something, on a large scale, that we’d sworn not to. Most of us felt as though we were violating Executive Order 12333.”

That order, issued by President Ronald Reagan in 1981 in response to the Church Committee’s extensively documented findings on illegal domestic surveillance and plots to kill foreign leaders, banned the U.S. government from planning or carrying out assassinations. But government lawyers do not interpret “assassination” as a synonym for “targeted killing” when it relates to terrorists, a distinction predating Washington’s conflict with al Qaeda. Similar concerns about targeted killings arose after the 1983 bombing of the U.S. embassy in Lebanon. In that case, as the journalist Walter Pincus later reported for *The Washington Post*, CIA discussions produced “an informal agreement with the congressional oversight committees that if a covert action targeted a terrorist in his apartment plotting to blow up a building, he had to be detained. But if the terrorist were found and known to be on his way to blow up a building . . . he could be killed if that were the only way to stop him.” And as the executive order notes, the intelligence community is charged with conducting “special activities” to protect national security, a category under which the drone program falls.

Even so, senior officials remain uncomfortable with the CIA’s growing paramilitary role, which Brennan himself described during his February 2013 confirmation hearing as an “aberration” from the agency’s traditional focus on espionage. In fact, soon after Brennan took the CIA’s helm, the White House looked poised to shift all drone warfare to the Pentagon, which has its own drone program. Yet the move never happened, in part because the generals balked and Congress couldn’t bypass its own committees’ stovepiping. The most important factor, however, was the CIA’s success. As Michael Hirsh, writing for the *National Journal*, noted in February 2014, experts believe that the CIA “may simply be much better than the military at killing people in a targeted, precise way—and, above all, at ensuring the bad guys they’re getting are really bad guys.”

No public data are available to compare the CIA’s and the Pentagon’s drone programs, but the agency’s has earned high marks from senior policymakers. Months before a Pentagon drone strike reportedly hit a convoy that included innocent Yemeni wedding guests in December 2013, Democratic Senator Dianne Feinstein of California, then chair of the Senate Intelligence Committee, praised the CIA’s “patience and discretion” and raised concerns that “the military program has not done that nearly as well.”

Critics of keeping a drone program under the CIA’s roof contend that the agency’s primary mission should be espionage rather than covert action. There’s no reason, the argument goes, that the Defense Department could not develop its expertise in carrying out secret drone strikes and other deniable operations over time. Shifting all drone warfare from the CIA to the Pentagon would also be perfectly legal; the president could put pen to paper and authorize it tomorrow.

The problem, however, is that a central mission of the CIA—developing human intelligence—is getting much tougher to carry out. To some extent, that is due to the makeup of the agency's own work force. Although the CIA now selects from a wider pool than it once did (when its ranks were, as it was said, mostly pale, male, and Yale), the government's clearance system still freezes out qualified applicants—even those with critical language skills and cultural acumen—for having a grandmother in Baghdad or an uncle in Tunis. Penetrating tribal and nonstate groups in the Middle East is difficult enough as it is; doing so with few who understand Arab customs or speak a variety of Arabic dialects only adds to the danger.

Another factor making human intelligence gathering a harder game to play is the broader American political culture. Developing informants (let alone embedding assets) within terrorist groups is a dicey proposition. And regardless of their personal courage or willingness to serve, intelligence officers must now operate in a political climate that discourages risk taking, because the American public reacts so strongly to U.S. casualties—something the fallout from the 2012 attack on the U.S. compound in Benghazi, Libya, which killed two Foreign Service officers and two security personnel, made clear. Of course, such political constraints and risk aversion affect the U.S. military, too. This is partly why many U.S. policymakers are cool to the idea of putting boots on the ground in the fight against ISIS. The irony is that an effective air war relies on precise targeting, which requires good intelligence collected on the ground, which itself exposes U.S. personnel to the sorts of risks an air war is supposed to avoid.

Public controversy has also imperiled another source of human intelligence: interrogations. The Senate Intelligence Committee's multiyear investigation into Bush-era interrogation and detention programs has added fuel to the fire, challenging not only the legality of so-called enhanced interrogation techniques but also their effectiveness. (In 2003, as a member of Congress, I questioned the program's policy guidance and urged the CIA not to destroy videotapes of interrogations in a letter to the agency's then general counsel, Scott Muller.) For now, President Barack Obama's efforts to close the U.S. detention facility in Guantánamo Bay, Cuba, and move the terrorist suspects to domestic prisons have been hamstrung by congressional opposition to holding their trials in the United States. That said, the facility's prison population has shrunk from over 600 in 2003 to just 127 as of this writing. All eyes are on the next defense secretary to finish the job before Obama's term ends.

If these trends continue, they will make it difficult for the CIA to do much of the human intelligence collection it did in the past. So what should the intelligence community do? It could outsource some human collection to friendly foreign intelligence services that are less risk averse and better culturally equipped, such as those in Israel, Jordan, and the United Kingdom. The CIA could also focus its own collection on directly supporting covert operations. And it could continue to improve its security clearance process, making it easier, for example, to give temporary or limited clearances to individuals with sorely needed expertise.

But in today's environment, the CIA's main value added is reflected in its finances. According to a leaked copy of the intelligence community's "black," or classified, budget for 2013, reported in *The Washington Post*, funding for covert action programs ($2.6 billion) has outstripped funding for human intelligence ($2.3 billion). Follow the money, and one arrives at a basic fact: the CIA's edge is paramilitary.

DATA MINEFIELD

The CIA is not the only intelligence agency facing challenges. In the wake of the Snowden leaks, the media have depicted the NSA as an all-powerful agency with a limitless appetite for personal data and few barriers to getting it. In an ongoing debate, civil liberties advocates have faced off against national security hawks, with both sides sharing a single flawed assumption: that the NSA's competitive advantage is in the mass collection of data.

In fact, the NSA's digital dragnet has never been as sweeping as its most vocal critics like to insinuate, and Congress amended FISA in 2008 to ensure that the agency's data collection was carefully circumscribed and reviewed by the Foreign Intelligence Surveillance Court. What's more, new proposals to limit the NSA's programs further are gathering steam, and U.S. technology firms are taking increasingly dramatic steps to protect their customers' data.

Indeed, the NSA's future will be shaped, more than anything else, by its relationship with Silicon Valley—one in which the agency is fast becoming the junior partner. One can doubt the sincerity of the technology community's outrage over the NSA's surveillance practices—doubt, for example, that the Facebook co-founder Mark Zuckerberg, whose company reportedly stores petabytes' worth of data about its billion-plus active monthly users, was shocked at the thought of mass data collection. But Silicon Valley's reaction has bite, and the outcome has been an encryption drag race that has top government officials panicking. Rather than fight surveillance policies in court, where the government has an overwhelming edge, companies such as Apple, Facebook, and Google have responded in cyberspace. To satisfy a global customer base with strict privacy expectations, they've developed technical capabilities to put customer data under lock and key.

Apple now dedicates a section of its website to "government information requests," which isn't a page about how cheerily they comply. "Our commitment to customer privacy doesn't stop because of a government information request," it reads. Apple iPhones running the latest operating system, iOS 8, have their data encrypted and hidden behind a passcode that makes it, in Apple's words, "not technically feasible for [Apple] to respond to government warrants for the extraction of this data." Google has followed suit, adding a similar function to Android phones. Other agencies are feeling the ripple effects. Last October, James Comey, the director of the FBI, said that the bureau was "struggling to . . . maintain [its] ability to actually collect the communications [it is] authorized to collect."

For years now, there has been a growing gap between the technical capacity of the public sector and that of the private sector. Like the CIA, the NSA has a recruitment problem. The agency lies on the wrong side of a generational divide on privacy; it also has no hope of matching the stratospheric salaries that firms such as Facebook offer even their interns. The security clearance system has made matters worse, putting candidates through the wringer over marijuana use and illegal music downloads. Some NSA hiring practices have improved, but no one expects that the agency will be able to outcompete technology firms for top talent anytime soon.

Over the long run, then, Washington won't win a digital competition with Silicon Valley. And now that the government needs the private sector more than the private sector needs it, the most important task is to rebuild trust between the two. True, the NSA could look for ways to get around technology companies' defenses, but any botched attempts would carry a high

political cost. Instead, the agency needs to keep serving warrants through the front door, abide by established legal procedures, and work to persuade the public of its respect for privacy. As companies such as Facebook and Google become more deeply integrated into global communications infrastructure—both are reportedly looking into providing Internet services to the developing world—they could become partners with the government in open-source data collection. That joint effort, if FISA-compliant and properly explained to the public, would be a gold mine for low-cost intelligence collection. But the intelligence community needs to make a savvier, more respectful pitch to the private sector, one that recognizes the digital balance of power. The goal should be to turn privacy and security into a positive-sum game: to guarantee more of both.

What role does that leave for the NSA? Its top priorities should be code-making, code-breaking, and cyberwarfare. Washington will still need the capacity to penetrate secure state networks and prevent its enemies, state and nonstate, from doing the same. Although the NSA has demonstrated abilities in this sphere, it needs to focus on keeping pace with talented Chinese, North Korean, Russian, and nonstate hackers.

IN PLAIN SIGHT

The rising power of Internet companies has paralleled another force upending the world of intelligence: the exponential growth of open-source information. During the Cold War, nothing could match the value of a well-placed mole or a thoroughly bugged bedroom. Today, the so-called dip party, where spies would eavesdrop over cocktails, has gone the way of the dodo. That's in large part because much of the information policymakers seek is no longer secret. Although complicated tradecraft remains useful in some contexts—advanced cyberattacks rely on intimate knowledge of human beings, their habits, and their software use—the CIA doesn't need an agent in the Russian Ministry of Agriculture in order to follow developments in Ukraine. Social media, in fact, has provided some of the best reports from the ground, allowing bystanders to upload photographs and videos as events unfold in real time. Intelligence agencies need to take advantage of the technological revolution that allowed a Tunisian fruit vendor to spark the Arab Spring, that ISIS exploits by posting barbaric videos designed to attract thousands of followers, and that the State Department has begun to embrace on Twitter.

Now that every smartphone user is a potential collector of intelligence, the key is to skillfully sort the data. Although no structural obstacle prevents the U.S. intelligence community from doing this work well, there remains a strong bias, bordering on elitism, against using freely available information. Too often, the preference is to tap terrorists' phones and send spy satellites in search of hidden training camps, not to read the tweets of a 19-year-old jihadist. But in an era of online radicalization, indoctrination often happens in plain sight.

As the intelligence community moves away from traditional espionage and toward open-source analysis, one of the most important, enduring questions in the spy business will take center stage: how to protect analysis from being biased by policy preferences. Intelligence reform in 2004 was prompted in large part by just how badly the intelligence process went wrong in the lead-up to the U.S. invasion of Iraq in 2003 and before the 9/11 attacks in 2001. Policymakers rightly wanted—and still want—to ensure that the nation never faces anything like those failures again.

The reforms that Congress enacted in 2004 were the right ones for their moment. But now the terrain has shifted. When one

expands the intelligence base to include the vast reams of raw information widely available to anyone through open sources, there are infinite ways for individual pieces of data to bias policymakers before analysts can present the bigger picture. Of course, there have always been ways for bias to creep into the briefing process: through analysis that has been crafted with an eye toward specific policy prescriptions, for example, or through insistent briefings on a single topic that the president hasn't solicited. Open-source information will make the problem worse, but no reorganization or policy change will make it go away. People bring prejudices to everything they do; in the end, intelligence is only as good as the people who analyze it.

That basic fact won't change anytime soon, but much else will. To borrow from William Gibson, the novelist who gave cyberspace its name: "The future is already here—it's just not very evenly distributed." The trends shaping the intelligence community are detectable: in budgets, in organizational charts, and in war zones. Policymakers have been slow to notice, as their attention jumps from one crisis to the next. But if Washington wants to get ahead of the curve and anticipate future flare-ups, that needs to change. As in the past, people are not the problem; the country's analysts and officers continue to serve with courage and distinction. The challenge lies instead with a system that is less adaptable than the enemies it confronts, hobbled as it is by conventional thinking.