Good Intelligence Is a Key Ingredient to Good Foreign Policy

Jane Harman

For four decades, the Aspen Strategy Group has probed the day's tough foreign policy problems. This year's topic—Domestic and International (Dis)order—focused on reemerging threats, including China. How we understand the threats posed by China, Russia, jihadis, and the pandemic requires state-of-the-art intelligence. We need to know everything we can about capabilities, plans, and intentions in order to equip the president and our foreign policy team to make the best decisions. This paper focuses on the state of our intelligence. Too often, our conversations skip straight to the question of what we need to *do*, rushing past the question of what our decision-makers most need to *know*.

That kind of haste is costly, and regrettably common. Our country has repeatedly learned, and just as often forgotten, that you can't make good policy without good intelligence. Today, the intelligence function is as important as it's ever been, but the job is far harder to do well. In this golden age of misinformation, our adversaries hide their intentions beneath layers of bluff and double-bluff, speaking through a thousand masks and cut-outs. Across portfolios—whether in the Middle East or the digital domain—the line between secret sparring and open conflict is thinner than ever. Is Russia probing our networks to collect intelligence, to shore up its own defenses, or to flip the switch on our power grid tomorrow? Is Iran trying to save face or moving to a bona fide war footing? Which of our negotiating partners is ready to strike a deal, and which to pick our pockets?

Meanwhile, over the last several administrations, our intelligence community has been hit by overlapping crises—wrong-footed by fundamental changes in the way spying works. We have moved from a world in which secrets were sparse, locked away in safes, to a world of too much information, in which truth hides in plain sight and signals are swamped by noise. We've left an era defined by the well-placed mole for one ruled by backdoors and deepfakes. In the process, hackers and technology firms have become as important to intelligence policy as governments—sometimes as instruments of the state, but just as often in the roles of rogue actors or contractors.

To be sure, at times Congress has found the political will to pursue serious oversight and reform of the intelligence community. In the Intelligence Reform and Terrorism Prevention Act of 2004, we created new institutions—such as the Office of the Director of National Intelligence (ODNI) and the Privacy and Civil Liberties Oversight Board (PCLOB)—to promote a transparent, accountable, better-coordinated intelligence community (IC). In the Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008, we brought the executive branch's secret spying programs under law and tried to create a sustainable framework for future surveillance. But many of these reforms have disappointed, while momentum to make further progress has stalled out. At home, Americans in both parties remain skeptical of the executive branch's commitment to observing legal boundaries. Abroad, our European allies remain profoundly unhappy with our zero-sum game between security and privacy—unhappy enough to threaten the free flow of information across the Atlantic.

As a result, we now face a difficult double game. Not only do we need to fix what's broken or obsolete in our intelligence community, we need others to trust that we've made repairs. Our challenges have deepened, sharpened, and multiplied.

Confronting Politics in Intelligence

The most dangerous threat to our intelligence function is also the oldest, as well as the hardest to stamp out: politicization. When we let the tail wag the dog, when the "right" answer has been picked out before our analysis ever gets going, we risk blinding ourselves to national security realities. We know the potential costs, of course, in the wake of the Iraq intelligence debacle, but every White House confronts some fresh temptation to forget the lesson. And while the issue has taken on a higher profile under this administration, the problem hardly started—and won't end—with this president. Making durable progress toward an independent intelligence community means taking a hard look at institutions, not just individual personalities.

After all, as long as we've had spy agencies, there have been individuals tempted to misuse them. Politics can creep in at any stage—when deciding where to point our collection tools in the first place, when choosing how to contextualize raw reports, and when deciding what makes it into the President's Daily Brief. But the problem is especially acute today, because the most important stage in our contemporary intelligence process is *analysis*. We don't live in a world of scarce intelligence anymore; instead, we risk drowning every day in a flood of raw information. There's always enough information to tell almost any story—enough unfiltered intelligence that, massaged properly, up can look like down, right like left, or a friend like an enemy. It can happen in a thousand subtle ways. Through selective briefing, or selective leaks, or selective declassification. By threading coincidences together into conspiracy. By mixing high- and low-quality sources to launder issues of credibility. At each stage, intelligence risks becoming just another branch of public relations.

Sometimes, politicization is a question of officials twisting the story that reaches the president to pursue some factional agenda or preconceived policy preference. But presidents, of course, have more than have enough tools on hand to push the boundaries themselves. They can manipulate the appointments process to install loyalists in key offices. They can manipulate their nearly plenary power over the classification process to conceal unflattering or inconvenient truths. And when one element of the intelligence community won't offer the right answer, there are fifteen more to shop around at. As often as these maneuvers have played out, the point we've yet to internalize is that all of these are *self*-sabotaging moves. Without unbiased analysis, a commander-in-chief is making foreign policy choices with blinders on. That's a movie we've all seen before, and a mistake we cannot afford to repeat.

Adapting Human Intelligence to a New World

The image of the spy at a "dip party" became obsolete by the end of the Cold War. Today, human intelligence (HUMINT) is no longer just gathering intelligence from human sources. That's partly because we have advanced tools and open sources—from satellites showing us images a man or a woman couldn't provide to reading what's in the newspaper or gleaning insights from the Islamic State's public Telegram channels—to supplement our collection efforts. But we still need humans to develop sources to carry out our most sophisticated cyber operations. It's a misconception that these operations happen at the speed of light; most are a long process involving reconnaissance and a lot of information, and we have to step away from the keyboard so that we can set up the circumstances for human targets to make a mistake. At the same time, we live in an age of extensive surveillance making it harder to operate in certain places, and policy makers, for their part, have only grown more risk-averse, ratcheting up the political cost of planting our people in dangerous positions.

Our adversaries' growing cyber capacity heightens the difficulty further. Because China and Russia are in our networks, they've seen our payroll—and that includes our spies, who need salaries and health insurance as much as any employee at the Department of Agriculture. Incidents like the hack of the Office of Personnel Management, or the data breaches at private firms like Anthem and Equifax, have scattered fragments of our officers' identities all over the world. Building covers that can stand up to that degree of digital scrutiny is extraordinarily difficult, shading into impossible. And the politicization of intelligence throws yet more fuel on the fire. No one will sign up for a dangerous undercover role if their identity might be declassified for partisan gain down the road. No ally will share secrets from a well-placed source if we can't swear to keep them.

None of these trends is likely to shift to the advantage of human spies any time soon. Instead, at IC components like the Central Intelligence Agency, we need to rebalance our investments to reflect what they can still do well. As I've argued before, the agency has developed an impressive capacity for kinetic action and support. Even as the most urgent threats confronting us shift—from non-state organizations to near-peer competitors—that expertise will remain invaluable in tomorrow's gray-zone conflicts. But making the change will require shaking loose from an organizational culture that is rooted in the Cold War, which ended over three decades ago.

Signals Intelligence in the Shadow of Silicon Valley

Though in some respects our signals intelligence (SIGINT) efforts are cutting edge, in others they risk becoming outmoded even faster than our HUMINT undertakings do. The most volatile variable in the mix, though, isn't the obsolescence of any particular gizmo—it's Washington's always-evolving relationship with the tech giants in Silicon Valley. Our government has been slow to grasp that the business decisions made by a handful of private firms influence our access to intelligence as much as any bill passed by Congress or any executive order. We've been slow to understand, too, that when we fail to establish accountability guardrails of our own, other parties will throw up walls of their own, jeopardizing our access to information in the long run.

Over the last ten years, for instance, nothing has damaged our SIGINT capacity more than our initial insistence on "collecting it all." We now know that some of the most expansive undertakings of the Bush and Obama administrations, like the telephone metadata program that operated under Section 215 of the PATRIOT Act, produced little actionable intel. Pending legislation to curb practices has stalled in Congress, which is only further complicated by some alleged FISA application missteps at the Department of Justice.

We'll be living with the consequences for the foreseeable future because Silicon Valley reacted by "encrypting it all." We lost access not only to what we *shouldn't* have been able to collect, but also to data that once would have been subject to ordinary warrants and valid legal process—all with the flick of a switch. Now, that shift may turn out to have been for the better; the gains to our cybersecurity may ultimately outweigh the intelligence we forfeited. But regardless, the experience should have been a sharp lesson learned.

It didn't take. Law enforcement has picked fight after fight with the tech giants, pushing Apple and others to adopt ever more elaborate technical safeguards—and pushing more and more of our intelligence targets onto high-security platforms. This is an arms race we can't win; it's imperative we stop trying before we do any more damage. Instead, of course, technology policy is becoming more and more of a political football, the kind of Washington conversation in which the people who know the least talk the loudest. And the rift is deepening at a moment when technical capacity has never seemed more critical to our national security future. Who's going to have the edge in the race to develop powerful artificial intelligence: the countries that celebrate their whiz kids or the countries that marginalize and antagonize them? Where are the next big leaps in quantum computing—or in quantum-proof cryptography—going to come from?

A twist on the same dynamic has played out in our relationship with Europe. Some of our allies have never fully gotten over Edward Snowden's disclosures; some of them don't think very highly of the reforms we've taken in response. We could go back and forth over whether that reaction is justified, but the reaction is real, and it threatens severe consequences for the free flow of information across the Atlantic. Just this summer, the Court of Justice of the European Union threw out the Privacy Shield agreement, which lets firms transfer data from Europe to the United States, on the theory that American law doesn't do enough to protect its citizens against our intelligence agencies. That decision has been criticized (fairly) for overstating the difference between the European and American approaches to national security surveillance. But whatever its merits, the ear-splitting alarm is worth hearing: if the United States fails to set more appropriate limits on National Security Agency (NSA) data collection, Europe will set its own. And if the EU pursues the kind of "data sovereignty" Russia and China have pioneered, the consequences for the open internet—not to mention our intelligence partnerships—could be disastrous. In the long run, we lose far more by pushing our partners' privacy boundaries than we do by showing we respect them.

Where We Need to Go

It would take a book to explore every patch, fix, and reform, and even that magnum opus would be incomplete; these challenges are *dynamic*. Addressing them will take leadership—in Congress, in the White House, and in the senior ranks of the intelligence services. Still, my short list of prescriptions has to begin with remedies for politicization.

Of course, there is no single silver bullet. Instead, we'll have to create overlapping accountability mechanisms, safety nets that back each other up. For one, we need to update the Federal Vacancies Reform Act to ensure that Congress keeps its say in who fills the nation's top spy jobs. The responsibility to advise and consent is a grave one, not to mention a powerful oversight tool, but it comes to nothing if the president can shuffle appointees around the bureaucracy without needing to send anyone to the Hill for Senate approval. In the same spirit, we need to strengthen protections for the inspectors general (IGs) who help make sure the intelligence community colors within the lines. When IGs are removable at a moment's notice, a determined president can end any investigation or report with a phone call—paying little to no political cost in the process. Congress must likewise insist that the president properly staff and empower watchdogs like the Privacy and Civil Liberties Oversight Board. The PCLOB's reports have been an indispensable source of ground truth on our intelligence programs—for one, the agency concluded that the metadata program raised legal concerns long before the courts did—but the agency is defanged when it lacks a quorum, as it did for too long in the Trump administration.

By the same token, the intelligence community must learn to tolerate greater scrutiny and transparency if it hopes to regain the trust of partners and the public. The Foreign Intelligence Surveillance Court (FISC), for instance, has lost the trust of too many parties to continue on with business as usual. We need to let sunlight in to reassure members of both parties that surveillance powers are being exercised appropriately (not politically) and to make clear that the executive hasn't returned to the bad old days of secret law. That means publishing more of the FISC's legal determinations; it means expanding the participation of amici curiae, who can ensure civil liberties are taken seriously. The executive branch must also make sure that criminal defendants receive the notice they're entitled to—under both our intelligence statutes and the Constitution—when the fruits of foreign surveillance are used against them at trial. Reforms like this would help reassure the world that our intelligence programs are subject to judicial review and that we're confident they can pass with flying colors.

Only by regaining the public's trust—and only *when* we've regained the public's trust—can we put our spy agencies on a sustainable footing for the future. And only with good intelligence can we hope to craft the foreign policy we need.

Jane Harman is the Director, President & CEO of the Wilson Center and a former nine-term member of Congress from California. She served as Ranking Member of the House Permanent Select Committee on Intelligence from 2003 to 2007; was a principal author of the Intelligence Reform and Threat Prevention Act; and was deeply involved in the government's response to the September 11 attacks. Since joining the Wilson Center, she has served on advisory boards to the Central Intelligence Agency, the Office of the Director of National Intelligence, and the Departments of State and Homeland Security. She also currently serves on the Defense Policy Board. She is teaching a seminar at Harvard Law School, her alma mater, and has a book forthcoming in May 2021. She is a trustee of the Aspen Institute and a member of the Aspen Strategy Group.