3

I Spy a Problem

Transforming US Intelligence Agencies for the Technological Age

Amy Zegart

This paper examines the adaptation challenges of US intelligence agencies today with an eye toward a crucial question: How much does money matter? The short answer is that nobody really knows, but it's probably less than we think. The US Intelligence Community (IC) failed to adapt to the rising terrorist threat in the 1990s, when intelligence budgets were cut dramatically after the Cold War, and the IC is also struggling to adapt to the technological age today, when intelligence budgets have never been higher. When budget scarcity and abundance lead to the same suboptimal outcome, something more systematic is likely at work. Its name is organizational pathologies. To be sure, higher spending certainly can help shift intelligence priorities and deliver new capabilities. And reduced spending can hurt. But I find that organizational features of intelligence agencies are often silent but deadly killers of innovation. Agency structures, cultures, and career incentives critically shape what is valued, what gets done, and how well. Unless these organizational features are aligned more rapidly with the threat landscape, intelligence agencies will struggle to deliver timely insights to policy makers no matter how much funding they have.

The first section of this chapter issues a cautionary note about the difficulties of analyzing the relationship between intelligence spending and

The views expressed in this chapter are solely those of the individual author and do not necessarily reflect the views of any organization with which they are, or have been, affiliated.

An earlier version of this paper appeared in *Foreign Affairs*. See Amy B. Zegart, "Open Secrets: Ukraine and the Next Intelligence Revolution," *Foreign Affairs* 102, no. 1 (December 20, 2022; January/February 2023): 54–71.

performance outcomes, offers a broad overview of declassified intelligence budgets over time, and examines how organizational weaknesses were the root cause of intelligence failures leading to 9/11. The second section examines how in a range of policy areas—from health care and K–12 education to defense—greater spending is not producing better results. I then turn to intelligence, arguing that despite record spending, US spy agencies are losing their relative advantage today. Thanks to the rise of emerging technologies and the explosion of data, intelligence isn't just for superpower spy agencies anymore. The third section concludes with what can be done, starting with the creation of a new dedicated open-source intelligence agency.

Breadcrumbs and Budgets

At the outset, it's worth underscoring that studying anything in intelligence is tricky business, because the public record is so incomplete. It's hard to identify the causal factors that lead to success or failure when failures are often public but successes are often secret.

The impact of budgeting decisions is especially challenging. Intelligence spending is so highly classified that until 2007, with rare exceptions, even the topline total intelligence budget remained secret.[1] As a result, for years, expert analysts have estimated intelligence spending over time based on breadcrumbs of data from declassified reports and remarks by government officials.[2]

Since 2007, total intelligence spending in two major categories has been released annually. These are the National Intelligence Program (NIP), which covers programs, projects, and activities of the IC, and the Military Intelligence Program (MIP), which covers intelligence activities of military departments and agencies in the Defense Department that support tactical US military operations. In FY2022, the NIP was $65.7 billion, and the MIP was $24.1 billion, for a total intelligence budget of $89.8 billion.[3] Yet even this aggregate figure is incomplete. It excludes other specific intelligence-gathering programs in cabinet departments and agencies (such as Homeland Security) as well as military programs that include intelligence but have a different primary purpose—such as the MQ-9 Reaper unmanned aerial strike platform.[4]

More importantly, declassified intelligence budgets do not provide meaningful data to assess whether the eighteen agencies of the US Intelligence Community are deploying their resources against the right priorities, particularly as the threat landscape changes. How much does the US government spend by intelligence agency, activity, or capability? How much is spent on

understanding and countering nation-state actors like China and Russia versus transnational terrorists, the proliferation of weapons of mass destruction, or cyber threats? Is the IC dedicating sufficient resources to attracting and retaining the right STEM talent? We don't know. There are, of course, good national security reasons for not making this kind of information publicly available. My point is that analyzing the efficiency or effectiveness of intelligence spending from the outside is an exercise in speculation. Humility is in order.

Here's what we do know: In broad-brush terms, spending for US intelligence increased significantly during the Cold War, declined by approximately 20 percent during the 1990s, and skyrocketed after 9/11. Figure 3.1 is an

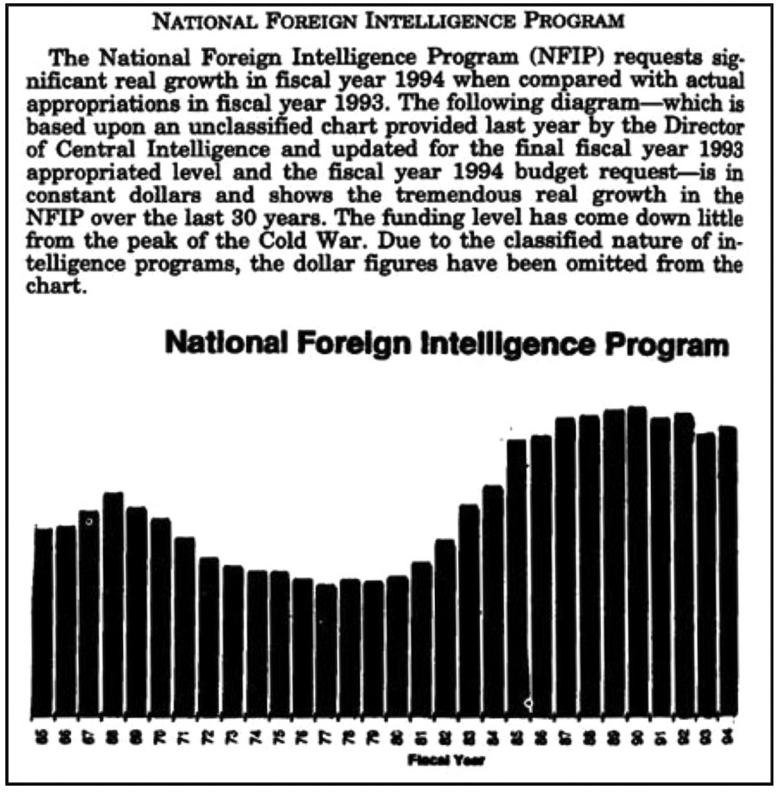

Figure 3.1 Intelligence Spending, 1965–94 (in 1994 constant US dollars)

Source: From H.R. Rep. No. 103-254, Department of Defense Appropriations Act, 1994, to accompany H.R. 3116, reproduced in Michael E. DeVine, "Intelligence Community Spending: Trends and Issues," Congressional Research Service Report R44381, updated June 18, 2018.

unclassified chart released by a 1994 House report showing spending trends from 1965 to 1994 (note all actual numbers were omitted). The House report describes Cold War spending as experiencing "tremendous real growth" over thirty years.

The Soviet Union's collapse in 1991 brought dramatic reductions to intelligence and defense budgets, which lawmakers dubbed the "peace dividend." Some, including Senator Daniel Patrick Moynihan, argued that the CIA should be abolished, because it was no longer needed. According to former director of national intelligence James R. Clapper, in the 1990s, the IC experienced a 23 percent budget reduction, creating a "damaging downward spiral."[5] Director of Central Intelligence George Tenet told the 9/11 Commission that during the 1990s, the entire IC lost 25 percent of its workforce, the CIA suffered a 16 percent workforce decline, and the agency's budget declined by 18 percent in real terms. "This loss of manpower was devastating," noted Tenet, "particularly in our two most manpower intensive activities: all-source analysis and human source collection. By the mid-1990s, recruitment of new CIA analysts and case officers had come to a virtual halt. NSA [National Security Agency] was hiring no new technologists during the greatest information technology change in our lifetimes."[6] The real picture was even worse than these numbers suggest, because personnel reductions were made through voluntary attrition rather than targeted cuts to retain top talent, weed out poor performers, or ensure key skill sets and geographic and functional areas were well covered.[7]

Declining budgets undoubtedly made it difficult for the IC to adapt to the rising terrorist threat in the years before the September 11, 2001, terrorist attacks. Yet evidence suggests there's much more to the story than shrinking resources. I find that the roots of the failure to prevent 9/11 lay in broader, deeper organizational weaknesses in US intelligence agencies that had surprisingly little to do with funding. Throughout the 1990s, even as America's spy agencies warned of the growing terrorist danger, they remained stuck in their Cold War posture, operating with organizational structures, cultures, and career incentives that offered little chance of stopping al-Qaeda from committing the worst terrorist attack in American history. My five-year examination of thousands of pages of declassified documents and interviews with seventy-five current and former intelligence and government officials found that the CIA and FBI had twenty-three opportunities to penetrate and possibly stop the 9/11 plot. Organizational weaknesses led to failure every time.[8] Below are thumbnails of two such lost opportunities.

The CIA's Watchlisting Failure

The 9/11 Commission and the Congressional Joint Inquiry both suggest that perhaps the best chance to stop the 9/11 attacks involved the travel of two al-Qaeda operatives named Khalid al-Mihdhar and Nawaf al-Hazmi. Both men were part of the team that crashed American Airlines Flight 77 into the Pentagon.

They first tripped the wire in January 2000, when they attended a secret al-Qaeda meeting in Malaysia. The CIA was watching. The agency got a photograph of al-Mihdhar, learned his full name, obtained his passport number, and uncovered that he held a multiple-entry US visa. By March 2000, CIA officials identified al-Hazmi as having attended the same meeting, learned his full name, and discovered he had already entered the United States. Between fifty and sixty CIA officials had access to this information about al-Mihdhar and al-Hazmi. And yet nobody put these two men on the State Department's watchlist denying them entry into the United States or notified the FBI for the next year and a half.[9] Why?

The simplest answer is that the CIA had never been in the habit of watchlisting suspected al-Qaeda terrorists before. For more than forty years, the agency and the rest of the IC had operated with Cold War priorities, procedures, and thinking, all of which had little need to ensure dangerous foreign terrorists stayed out of the United States. Before 9/11, there was a watchlisting program in name but not in practice: there was no formal training, no clear process, and no priority placed on it.[10] As one CIA officer told congressional investigators after 9/11, he believed it was "not incumbent" even on the CIA's special Osama bin Laden unit to place people like al-Mihdhar on the State Department's watchlist.[11]

The FBI's Failed Search for Two al-Qaeda Operatives

On August 23, 2001, just nineteen days before 9/11, the CIA finally told the FBI that al-Mihdhar and al-Hazmi were probably in the United States and needed to be found. The FBI responded by putting the search for these two suspected terrorists at the bottom of the priority list and handing it to the C-team. The "nationwide" hunt was the focus of just one of the bureau's fifty-six US field offices. It was designated "routine," the lowest level of priority. And it was assigned to a junior agent who had just finished his rookie year and had never led this kind of investigation before.[12]

Here too, organizational pathologies, not individual screwups, were to blame. The bureau dedicated just one office to what should have been a

nationwide search, because the FBI had always been a decentralized organization where each field office operated largely autonomously—and that's how all cases were handled. Putting one office on each case made sense for catching criminals after the fact and tailoring priorities to local law enforcement needs. It was a poor organizational setup for collecting and coordinating intelligence about future national security threats to the nation as a whole. Culture explains why finding al-Mihdhar and al-Hazmi went to the bottom of the pile. Although the FBI's own strategic plan declared counterterrorism its number one priority in 1998 and resolved to improve its domestic intelligence capabilities, the bureau was first and foremost a law enforcement organization with a culture that prized catching perpetrators of past crimes far more than gathering intelligence to stop a possible future tragedy.[13] In fact, a Justice Department investigation found that before 9/11, intelligence analysis was considered so unimportant, the vast majority of FBI analysts were rated unqualified to do their jobs.[14] Promotion incentives reflected this culture. Handing the search to a junior agent wasn't a mistake; it was how things were supposed to work. Convictions made careers, so finding two potential terrorists who hadn't yet committed a crime and might never do anything illegal went to one of the office's least experienced investigators, because it was one of the least desirable jobs.[15] In short, the bureau's decentralized structure guaranteed that the alarm would be sounded only in one place. Its law enforcement culture ensured the alarm would be muffled by criminal cases and priorities. And incentives promised that someone with the least experience and expertise would be answering the call.

We now know that Khalid al-Mihdhar and Nawaf al-Hazmi should not have been hard to find. For months before the attack, they hid in plain sight in San Diego, using their true names on everything from rental agreements and credit cards to a California ID card and the telephone directory. They even contacted several targets of FBI counterterrorism investigations, at one point living with an FBI informant—all unknown to the FBI. The two al-Qaeda operatives didn't need secret identities or clever schemes to succeed. They just needed the CIA and the FBI to operate as usual.[16]

In short, while declining intelligence budgets in the 1990s certainly reduced the CIA's workforce and forced intelligence leaders to tackle a new problem set with fewer resources, the roots of failure on 9/11 appear to go deeper. Consider the counterfactual: If the CIA and FBI had unlimited resources in the run-up to 9/11, would they have succeeded in watchlisting and finding Khalid al-Mihdhar and Nawaf al-Hazmi before it was too late?

More Money, More Problems

Twenty years later, intelligence agencies now face a much more favorable budgetary environment, and yet they are struggling again to adapt to a shifting geopolitical landscape—driven this time by emerging technologies that are disrupting every facet of the intelligence enterprise. Despite record spending over the past two decades, intelligence agencies are losing their relative advantage.

The US intelligence budget has increased dramatically since 9/11, jumping from an estimated $60.37 billion in FY2001 to $89.8 billion in FY2022 in constant 2022 dollars—an increase of 49 percent over twenty years (see fig. 3.2).[17] Although budgets dipped in the period of 2010 to 2015, the broader historical pattern is growth. Indeed, the Congressional Research Service estimates that intelligence spending quadrupled from 1980 to 2010 in real terms.[18]

In policy areas, from health care to K–12 education to defense, increased government spending has not translated into better results. A 2021 study compared eleven of the world's richest countries and found that the United States spent the highest percentage of GDP on health care yet ranked last in affordability, access, and outcomes, including infant mortality and life expectancy at age sixty.[19] Economist Eric Hanushek has found that US K–12 education spending per pupil quadrupled from 1960 to 2017 in constant dollars. Yet student scores on national tests estimating achievement across subjects remained flat. American student performance on international tests also

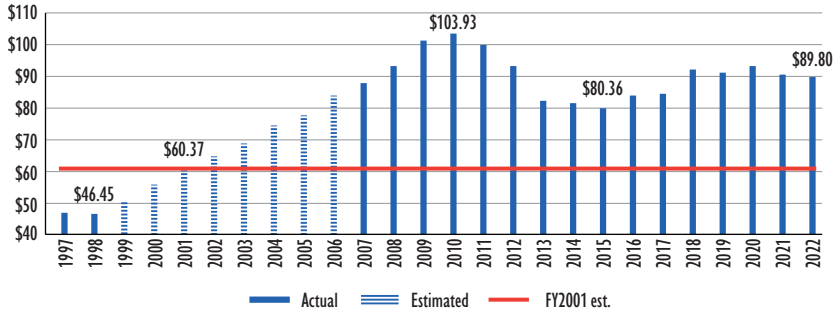

Figure 3.2 Total Intelligence Community Budget (constant $US billions)

Sources: Data for 1997 and 1998 from Steven Aftergood, "CIA Discloses FY1998 Intelligence Budget Total" (accessed December 7, 2022); data for 2007 to 2022 from Office of the Director of National Intelligence, "US Intelligence Community Budget." See endnote 17 of this chapter for an explanation of the author's analysis for 1999–2006.

remains persistently poor, and racial and income gaps have persisted.[20] And if the air force is any guide, bigger defense budgets have also not translated into better military readiness. While air force budgets have fluctuated since the 1980s, the number of air force aircraft, personnel, and other measures of end strength have all gradually declined.[21] In 2021, House Armed Services Committee chair Adam Smith publicly called the F-35 Joint Strike Fighter—a fifth-generation fighter jet riddled with technical deficiencies, which was the most expensive weapons program in history and ten years behind schedule—a "rathole."[22] The United States is estimated to spend more than the following nine countries in terms of defense budgets combined, and yet China's relative defense advantages are growing.[23] In short, American taxpayers seem to be getting less bang for their buck across various policy areas.

Increased intelligence spending after 9/11 produced arguably better outcomes than in these other policy areas, enabling the US to prosecute the War on Terror and defend the homeland to great effect. Changes included creating the National Counterterrorism Center and the Office of the Director of National Intelligence, an expanded drone program, and tighter integration between intelligence and military counterterrorism operations. As a result of these and other measures, the United States has not suffered another major catastrophic terrorist attack on American soil.

However, the dramatic infusion of counterterrorism funding also ended up hard-wiring the bureaucracy to fight the last war. Great-power competition, not transnational terrorism, now tops the threat list. And as I discuss more below, emerging technologies are transforming both the future and how intelligence agencies go about understanding it. This is a moment of reckoning for American spy agencies. And it reveals the paradox of plenty: surging budgets led to wide-scale changes, but by the time US intelligence agencies mastered the al-Qaeda problem, al-Qaeda wasn't the problem anymore.

The Tech Moment of Reckoning for Intelligence

Never before has the world stood at the cusp of so many technologies transforming so much so fast. Internet connectivity has transformed global commerce and supercharged global politics, fueling protests like the Arab Spring and Hong Kong's Umbrella Movement, empowering a new wave of government techno-surveillance led by Beijing, and enabling massive Russian deception operations to influence elections and undermine democracies from within. It's easy to forget how rapidly the internet has developed and how revolutionary it's been. In the early 1990s, less than 1 percent of the global

population was online. Now nearly two-thirds of the world is connected to the internet.[24] In the last three years alone, more than a billion people have come online.[25]

Artificial intelligence (AI) is also disrupting nearly every industry and changing how wars are fought—automating everything from logistics to cyber defenses to unmanned fighter jets that can overwhelm defenses with swarms and maneuver faster and better than human pilots. Some estimate that AI could eliminate up to 40 percent of jobs worldwide in the next fifteen years.[26] Russian president Vladimir Putin has declared that whoever leads AI development "will become the ruler of the world," and China has made no secret of its plans to lead the world in AI by 2030.[27] AI has been likened to electricity: a foundational technology that affects everything.

Technology is also revolutionizing the ability of humans to detect events unfolding on Earth from space. Commercial satellite capabilities now offer eyes in the sky for anyone who wants them. The number of satellite launches more than doubled between 2016 and 2018.[28] Today, more than five thousand satellites are orbiting Earth, and the Paris-based firm Euroconsult estimates that seventeen thousand satellites will be launched in the next decade.[29] While US spy satellites have more sophisticated sensing capabilities, commercial satellites are rapidly improving.[30] Some have resolutions so sharp they can detect manhole covers, signs, and even road conditions from space.[31] Others can detect radio frequency emissions, observe dynamic activities like vehicle movement and nuclear cooling plumes, and operate at night, in cloudy weather, or through dense vegetation and camouflage. Constellations of small satellites are offering something new: faster revisit rates over the same location multiple times a day so that changes can be detected over shorter periods. In 1960, when a US CORONA spy satellite successfully delivered images of the Soviet Union for the first time, the CIA's deputy director for science and technology, Albert "Bud" Wheelon, remarked, "It was as if an enormous floodlight had been turned on in a darkened warehouse."[32] Commercial satellites are turning that occasional floodlight into a continuously running video.

That's not all. Advances in quantum computing could eventually unlock the encryption protecting nearly all the world's data. Synthetic biology enables scientists to engineer living organisms with the potential for revolutionary improvements in food production, medicine, data storage, and weapons of war.

Perhaps most important from an American national security perspective is that nearly all of today's emerging technologies are invented outside the

government, made available to the world, and have widespread applications for commerce and conflict. That's new.

In the Cold War, breakthroughs like the internet and GPS were invented by US government agencies and later commercialized by the private sector. Few technologies were inherently dual use, which meant they could be classified at birth and restricted forever to keep them out of enemy hands. Nuclear technology, for example, was born secret and stayed that way, limiting the proliferation of the world's most dangerous weapons.

Now the script has flipped. Technological innovations are more likely to be developed in the private sector, where they are funded by foreign investors, developed by a multinational workforce, and sold to global customers. Today's technologies are born open, not classified, and are widely available, not easily restricted. AI, for example, has become so widespread and simple to use that high school students with no coding background can make deepfakes—AI-generated fake videos that look and sound real. Already, deepfakes impersonating former US ambassador to Russia Michael McFaul have been used to dupe Ukrainian officials and undermine the Ukrainian war effort, prompting McFaul to tweet, "WARNING. Someone using the phone number +1 (202) 7549885 is impersonating me. If you connect on a video platform with this number, you will see an AI-generated 'deep fake' that looks and talks like me. It is not me. This is a new Russian weapon of war. Be careful."[33]

This reversal gives private-sector leaders new power and national security officials new challenges. American social media platforms now find themselves on the front lines of information warfare, deciding what's real and what's fake, what speech is allowed, and what is suppressed. Start-up founders are inventing capabilities that can be used by enemies they can't foresee with consequences they can't control. As the war in Ukraine rages on and great-power competition with China intensifies, companies and investors have to weigh their economic interests against the national interest in new ways. Meanwhile, US intelligence agencies are struggling to adopt critical new technologies from the outside and move at the speed of invention instead of the pace of bureaucracy. Increasingly, private-sector leaders have responsibilities they don't want, and government leaders want capabilities they don't have. Power isn't just shifting abroad. Power is shifting at home.

All these forces unleashed by emerging technologies create a moment of reckoning for America's intelligence agencies. If we think of intelligence as a competitive contest for insight, then the challenges arising from emerging

technologies become more clear. They fall into five core categories—the "five mores."

More Threats, Speed, Data, Customers, and Competitors

The first challenge is more threats. Today's threat landscape has never been more crowded, complicated, or fast moving. After spending nearly half a century countering the Soviet Union and two decades fighting terrorists, US leaders now confront a diverse multitude of dangers that place demands on intelligence, including transnational threats like pandemics and climate change; great-power competition with Russia and China; terrorism and other threats arising from weak and failed states; and cyberattacks that steal, spy, disrupt, destroy, and deceive at stunning speeds and scale.

The list isn't just longer. Thanks to technology, it's harder. Cyber threats operate in ways that make them far more consequential than they appear and far more vexing to understand, detect, and defeat than the threats of yesteryear. Cyberspace is not just another military battleground like air, land, and sea, where the old tools and rules apply.

For centuries, power and geography have been the mainstays of security. Countries with the most powerful militaries and the blessings of geography—like the two vast oceans separating the US from the world's dangerous neighborhoods—were more protected. Not anymore. In cyberspace, power brings vulnerability, because the most powerful countries tend to be digitally reliant. And there's no such thing as good geography online; anybody can inflict damage from anywhere.

The character of war is different, too. Physical warfare tends to involve big moves that generate big consequences. But cyberwarfare is a bleed-every-minute affair where small attacks add up to devastating damage before you know it. China has stolen its way to technological advantage one hack at a time, in what FBI Director Christopher Wray has called one of the greatest transfers of wealth in human history, and "the biggest long-term threat to our economic and national security."[34]

Russia's interference in the 2016 US presidential election showed that cyberattacks can hack minds, not just machines, polarizing societies and undermining democracies from within at speed and scale. Russia wrote the playbook on using American tech companies to turn Americans against one another. Today, China doesn't need it. The popular social media app TikTok is owned by Chinese firm ByteDance and has quickly amassed more than a

billion users, including an estimated 135 million in the US. That's 40 percent of the US population.[35] Alarm bells are ringing. Democrats and Republicans are worried that TikTok could enable the Chinese government to vacuum all sorts of data about Americans and launch massive influence campaigns that serve Beijing's interest under the guise of giving American consumers what they want. In a world of information warfare, where weapons don't even look like weapons, it's fair to say the threat landscape isn't what it used to be.

Second, technological advances are generating the need for more speed in intelligence. Intelligence must be timely to be useful, delivering information when policy makers need it—before a missile launches, a summit convenes, or the National Security Council makes a decision.

Timeliness has always been important, but the speed of relevance is accelerating. In the 1962 Cuban Missile Crisis, President John F. Kennedy famously had thirteen days to pore through intelligence and consider his policy options in secret after U-2 surveillance photographs revealed Soviet nuclear installations in Cuba. On September 11, 2001, President George W. Bush had less than thirteen hours from the time the first hijacked plane crashed into the World Trade Center to review intelligence about who was responsible and announce America's response to the world. Today, the time for presidents to consider intelligence before making major policy decisions may be closer to thirteen minutes or thirteen seconds, or it could already be too late, because cyber breaches are often discovered long after the damage is done. In December 2020, for example, cybersecurity firm FireEye detected a massive breach of the software firm SolarWinds. Like a bad horror movie, when officials rushed to survey the damage, they discovered that hackers from Russia's elite foreign espionage service had been inside the house for a very long time—penetrating US nuclear labs, the departments of Defense, State, and Homeland Security, and much of the Fortune 500 more than a year before anyone found them.[36]

Now breaking events and hot takes are flowing directly into the hands of policy makers with the touch of a button, putting greater pressure on intelligence agencies to speed up or get left behind. But moving too fast also carries risks. It takes time to vet source credibility, tap expert knowledge across fields, and consider alternative explanations. Without careful intelligence analysis, leaders may make premature or even dangerous decisions. The potential consequences of rash action became evident in December 2016, when a news story reported that Israel's former defense minister threatened a nuclear attack against Pakistan if Islamabad deployed troops to Syria. Pakistan's defense

minister, Khawaja Muhammad Asif, quickly rattled his own nuclear saber, tweeting, "Israeli def min threatens nuclear retaliation presuming pak role in Syria against Daesh. Israel forgets Pakistan is a Nuclear state too, AH."[37] The original story, including the Israeli threat, had been fabricated, but the tweet apparently went out before it was verified. Satisfying policy makers' need for speed while carefully collecting, vetting, and assessing intelligence has always been a delicate balance, but it's getting harder to strike.[38]

The third challenge is data. The volume of data available online has grown so vast that it's hard to fathom. According to the World Economic Forum, in 2019, internet users posted 500 million tweets, sent 294 billion emails, and posted 350 million photos on Facebook every day.[39] Google answers several billion queries a day.[40] Every second, the internet transmits about 1 petabyte of data—the equivalent of binge-watching movies nonstop for over three years.[41] Data accumulation shows no sign of slowing. Some estimate that the amount of Earth's data doubles every twenty-four months.

American intelligence agencies are struggling to keep up. Already, they are collecting far more information than humans can analyze effectively. In 2020, one soldier deployed to the Middle East was so concerned about the crushing flow of classified intelligence emails he was receiving that he decided to count them. He received ten thousand emails in 120 days. And that's just the classified information.

Fourth, who needs intelligence to protect American lives and interests is changing radically, too. Until now, intelligence agencies produced classified reports for people with security clearances who read them in secured facilities with guards outside. Increasingly, however, important decision makers live worlds apart from Washington, making consequential policy choices in boardrooms and living rooms, not just the White House Situation Room. Voters need intelligence about foreign election interference and influence campaigns. Big tech companies like Microsoft and Google need intelligence about cyber threats to and through their systems. Most of America's critical infrastructure, from energy companies to financial services firms, is in private-sector hands. They can't go it alone in cyberspace, either. And because cyber threats don't stop at the border, American security increasingly depends on sharing intelligence faster and better with allies and partners.

Serving a broader array of customers requires producing unclassified products and engaging with the outside world. For agencies used to operating in secret, this is an unnatural act. Important efforts are underway. In the fall of 2022, the CIA launched a podcast called *The Langley Files*. Its aim:

demystifying the agency and educating the American public. "At CIA, there are truths we can share and stories we can tell," each podcast begins.

There are now public service videos from intelligence agencies about foreign threats to US elections. The National Geospatial-Intelligence Agency has launched a project called Tearline, a collaboration with think tanks, universities, and nonprofits to create unclassified reports about climate change, Russian troop movements, human rights issues, and more. Public-private partnerships in cybersecurity used to be a one-way street where NSA and the FBI asked companies for information but rarely provided any. Those days have changed. In 2021, NSA began issuing joint cyber advisories with the FBI and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency detailing major cyber threats, exposing the entities behind them, and explaining how to shore up defenses against them. In October 2022, these agencies even released the technical details of the top-twenty vulnerabilities exploited by the Chinese government to hack into US and allied networks, along with detailed instructions about how to defend against them.[42] The US government is now also issuing advisories with foreign intelligence partners.

The success of this public-facing strategy has been on full display in Ukraine. It helped the United States warn the world about Russia's invasion and rally the West behind a fast response. It continues to frustrate Moscow. Most recently, after Washington revealed intelligence indicating that senior Russian military leaders were discussing using tactical nuclear weapons in Ukraine, Chinese president Xi Jinping issued a rare public warning against the "use of, or threats to use, nuclear weapons."[43] Xi's trumpeted "no limits" relationship with Putin suddenly had limits after all.[44]

The fifth challenge for intelligence agencies in the technological age is more competition. It used to be that government spy agencies were the only organizations capable of launching satellites, collecting information at scale, and analyzing global threats. Not anymore.

The explosion of online open-source information, commercial satellite capabilities, and automated analytics like AI enables all sorts of individuals and organizations worldwide to collect, analyze, and disseminate intelligence—often better and faster than governments can.

In the past several years, the amateur investigators of Bellingcat, which describes itself as "an intelligence agency for the people," have identified the Russian hit team that tried to assassinate a former Russian military officer named Sergei Skripal, living in the United Kingdom, and located supporters

of ISIS in Europe.[45] It also proved that Russians were behind the shootdown of Malaysia Airlines Flight 17 over Ukraine.[46]

Bellingcat is not the only civilian intelligence initiative. When the Iranian government claimed a small fire had broken out in an industrial shed under construction in 2020, two American researchers working independently and using only their computers and the internet proved that Tehran was lying—within hours. David Albright and Fabian Hinz quickly found that the building was actually a nuclear centrifuge assembly facility at Natanz, Iran's main uranium enrichment site.[47] The damage was so extensive that the fire may well have been caused by an explosion, raising the possibility of sabotage. In 2021, nuclear sleuths at the James Martin Center for Nonproliferation Studies in California used commercial satellite imagery to discover more than two hundred new intercontinental ballistic missile silos in China, a finding that could signal historic increases in China's nuclear arsenal.[48]

And in the past year, Russia's war in Ukraine has given rise to an array of experts wielding unclassified information to track daily events and offer longer-term analysis online, from the Twitter feeds of former US officials to the Institute for the Study of War, which even features an interactive map. At Stanford University, there are now open-source intelligence courses for undergraduates, and a major volunteer effort has produced a series of reports compiling and confirming human rights atrocities in Ukraine for the United Nations. The Stanford student team, led by former army and open-source imagery analyst Allison Puccioni, used commercial satellite thermal and electro-optical imaging, TikTok videos posted online, geolocation tools, and more. "Today, anyone and everyone can access reasonably credible first-hand reports of attacks leveled against Ukraine," says Puccioni. "These pictures or videos are informative in and of themselves. But when cross-checked against other forms of freely or cheaply available information like satellite imagery, they can be triangulated to calculate location and time-stamp of the event, creating something akin to the synthesized, multisourced insight of conventional classified intelligence."[49]

Open-Source Intelligence Is Having a Moment

For American intelligence agencies, open-source intelligence brings significant new opportunities as well as risks. On the positive side, citizen sleuths offer more eyes and ears around the world, scanning for developments and dangers as they arise. The wisdom of the crowd can be a powerful tool, especially for piecing together tiny bits of information. Open-source information

can be shared easily within government agencies, across them, and with the public, all without revealing sensitive sources or methods. As 9/11 showed, the barriers to sharing classified information are often too high, and the costs can be tragic.

But features are also flaws. Open-source intelligence is open to everyone, everywhere, regardless of their motives, national loyalties, or capabilities. Citizen sleuths don't have to answer to anyone or train anywhere. The line between the wisdom of crowds and the danger of mobs is thin, and small bits of information can deceive in big ways. After a 2013 terrorist attack on the Boston Marathon killed three people and wounded more than 260 others, Reddit users jumped into action. Posting pet theories, unconfirmed chatter on police scanners, and other crowdsourced tidbits of information, amateur investigators fingered two "suspects," and the mainstream media publicized the findings. Both turned out to be innocent.[50]

These weaknesses can create serious headaches for governments. When errors go viral, intelligence agencies have to burn time and divert resources fact-checking the work of others and reassuring policy makers about the job they were doing already and the assessments they had made before. Accurate open-source discoveries can cause problems, too. Findings, for example, can force leaders into corners instead of keeping things secret to make room for compromise and graceful exits in crises. To diffuse the Cuban Missile Crisis, for example, Kennedy agreed to secretly remove US nuclear weapons from Turkey if the Soviets took their missiles out of Cuba. Had satellite imagery been publicly available, Kennedy might have been too worried about the domestic political backlash to make a deal.

The Future of Intelligence: It's the Organization, Stupid

American intelligence leaders know that their success in the twenty-first century hinges on adapting to a world of more threats, more speed, more data, more customers, and more competitors. They have been working hard to get there—launching organizational reforms, technology innovation programs, and new hiring initiatives to recruit top science and engineering talent. But the challenges are hard, efforts have been piecemeal, and progress remains slow.[51] The rate of progress is especially concerning given that the challenges are well known, the stakes are high, and intelligence weaknesses have been festering for years. Multiple reports and articles have found that intelligence agencies are not keeping pace with technological developments.[52]

If I'm right, then Washington cannot address its present intelligence challenges by throwing more money at existing agencies. Instead, developing US intelligence capabilities for the tech age requires building something new: a dedicated, open-source intelligence agency focused on combing through unclassified data and discerning what it means.

Creating a nineteenth intelligence agency may seem duplicative and unnecessary, but it is essential. Despite Washington's best efforts, open-source intelligence has always been a second-class citizen in the US intelligence community, because it cannot overcome existing organizational structures, cultures, and incentives. Open-source intelligence has no agency with the budget, hiring power, or seat at the table to champion it. As long as open-source intelligence remains embedded in secret agencies that value secret information above all, it will languish. A culture of secrecy will continue to strangle the adoption of cutting-edge technology tools from the commercial sector. Agencies will struggle to attract and retain desperately needed talent to help them understand and use new technologies. And efforts to harness the power of open-source intelligence collectors and analysts outside government will fall short.

A new open-source intelligence agency would bring innovation, not just information, to the US intelligence community by providing fertile soil for the growth of far-reaching changes in human capital, technology adoption, and collaboration with the burgeoning open-source intelligence ecosystem. Such an agency would be a powerful lever for attracting the workforce of tomorrow. Because it deals with unclassified information, the agency could recruit top scientists and engineers to work right away without requiring them to wait months or years for security clearances. Locating open-source agency offices in technology hubs where engineers already live and want to stay—such as Austin, San Francisco, and Seattle—would make it easier for talent to flow in and out of government. The result could be a corps of tech-savvy officials who rotate between public service and the private sector, acting as ambassadors between both worlds. They would increase the intelligence community's presence and prestige in technology circles while bringing a continuous stream of fresh tech ideas back inside.

By working with unclassified material, the open-source agency could also help the intelligence community do a better and faster job of adopting new collection and analysis technologies. The open-source agency could test new inventions and, if they proved effective, pass them along to agencies that work

with secrets. The agency would also be ideally positioned to engage with leading open-source intelligence organizations and individuals outside the government. These partnerships could help US intelligence agencies outsource more of their work to responsible nongovernmental collectors and analysts, freeing up intelligence officials to focus their capabilities and clandestine collection efforts on missions that nobody else can do.

And there will still be many such missions. After all, even the best open-source intelligence has limits. Satellite imagery can reveal new Chinese missile silos but not what Chinese leaders intend to do with them. Identifying objects or tracking movements online is important, but generating insight requires more. Secret methods remain uniquely suited to understanding what foreign leaders know, believe, and desire. There is no open-source substitute for getting human spies inside a foreign leader's inner circle or penetrating an adversary's communications system to uncover what that adversary is saying and writing. Analysts with clearances will also always be essential for assessing what classified discoveries mean, how credible they are, and how they fit with other unclassified findings.

If history is any guide, the agencies, processes, and cultures that got us here will not get us there. The country faces a dangerous new era that includes great-power competition, a renewed war in Europe, ongoing terrorist attacks, and fast-changing cyberattacks. New technologies are driving these threats and determining who will be able to understand and chart the future. To succeed, the US Intelligence Community must adapt to a more open, technological world.

Notes

1. Office of the Director of National Intelligence (ODNI), "US Intelligence Community Budget," https://www.dni.gov/index.php/what-we-do/ic-budget (accessed December 7, 2022); director of Central Intelligence George Tenet released the FY1997 and FY1998 total intelligence budgets after Steven Aftergood from the Federation of American Scientists filed a Freedom of Information Act lawsuit, but Tenet then reversed course in FY1999. Subsequent toplines remained classified until 2007 when Congress mandated that the director of national intelligence disclose "the aggregate amount of funds appropriated by Congress" for the National Intelligence Program in Section 601 of the Implementing Recommendations of the 9/11 Commission Act (Public Law 110-53). Freedom of Information Act requests have produced some agency-level budget justification documents, but these are heavily redacted. See also Steven Aftergood, "CIA Discloses FY1998 Intelligence Budget Total," press release, Federation of American Scientists, March 20, 1998; Brian

Clampitt, "US Intelligence Budget Request Revealed," *Harvard National Security Journal*, February 23, 2011; "Intelligence Budget Data," Federation of American Scientists, https://irp.fas.org/budget (accessed December 7, 2022).

2. Marshall C. Erwin and Amy Belasco, "Intelligence Spending and Appropriations: Issues for Congress," Congressional Research Service Report R42061, September 18, 2013, 5.

3. ODNI, "US Intelligence Community Budget."

4. Anne Daugherty Miles, Michael E. DeVine, and Sofia Plagakis, "Intelligence Community Spending Trends," Congressional Research Service Report R44381, Version 16, updated January 9, 2023, 1–2.

5. James R. Clapper, "Current and Projected National Security Threats to the United States," Senate Select Committee on Intelligence, March 12, 2013, 9, https://www.intelligence.senate.gov/sites/default/files/hearings/11389.pdf.

6. Hon. George Tenet, "Written Statement for the Record, National Commission on Terrorist Attacks Upon the United States," submitted testimony for the eighth public hearing of the 9/11 Commission, March 24, 2004, 24, https://9-11commission.gov/hearings/hearing8/tenet_statement.pdf.

7. Amy B. Zegart, *Spying Blind: The CIA, the FBI, and the Origins of 9/11* (Princeton, NJ: Princeton University Press, 2007), 3, 73–74; Aspin-Brown Commission Final Report, "Chapter 9: The Need to 'Right-Size' and Rebuild the Community," March 1, 1996, 96–97.

8. Zegart, *Spying Blind,* 12.

9. Office of Inspector General, *OIG Report on CIA Accountability with Respect to the 9/11 Attacks*, June 2005, declassified August 2007, xiv, https://irp.fas.org/cia/product/oig-911.pdf.

10. Zegart, *Spying Blind*, 2.

11. Quoted in Eleanor Hill, "The Intelligence Community's Knowledge of the September 11 Hijackers Prior to September 11, 2001," statement before the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence Joint Inquiry, 107th Cong., 2d Sess., September 20, 2002, 8.

12. Zegart, *Spying Blind*, 156–57.

13. Federal Bureau of Investigation, *Draft FBI Strategic Plan: 1998-2003: Keeping Terrorism Safe*, unclassified version, May 8, 1998.

14. *Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001*, report of the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence, S. Rep. No. 107-351, H.R. Rep. No. 107-792, 107th Cong., 2d Sess., December 2002, 340.

15. Zegart, *Spying Blind*, 156–68.

16. Zegart, *Spying Blind*, 156–68.

17. FY2001 intelligence spending in nominal terms is estimated at $37.60 billion, based on the Congressional Research Service's 2013 report "Intelligence Spending and Appropriations: Issues for Congress" (Erwin and Belasco). This figure was then

inflation adjusted to $60.37 billion in 2022 dollars, using the Bureau of Labor Statistics' CPI Inflation Calculator, https://www.bls.gov/data/inflation_calculator.htm. Estimates for intelligence spending from 1999 through 2006 assume equal yearly increases between the unclassified 1998 and 2007 budgets and were also inflation adjusted using the Bureau of Labor Statistics' CPI Inflation Calculator. See Erwin and Belasco, "Intelligence Spending," 4–5; for FY2022, see ODNI, "US Intelligence Community Budget."

18. Erwin and Belasco, "Intelligence Spending," 5.

19. Eric C. Schneider, Arnav Shah, Michelle M. Doty, Roosa Tikkanen, Katharine Fields, and Reginald D. Williams II, "Mirror, Mirror 2021: Reflecting Poorly: Health Care in the US Compared to Other High-Income Countries," The Commonwealth Fund, August 2021. The eleven countries examined in the study were: Australia, Canada, France, Germany, the Netherlands, New Zealand, Norway, Sweden, Switzerland, the United Kingdom, and the United States. Health outcomes are a product of many causes, including underlying social and economic conditions. The study uses measures that focus more on outcomes likely to be affected by health care, such as life expectancy at age sixty rather than life expectancy at birth.

20. Eric A. Hanushek, "The Fall of Educational Productivity and Policy Paralysis," in *The Not-So-Great Society*, ed. Lindsay M. Burke and Jonathan Butcher (Washington, DC: Heritage Foundation, 2019), 45–51; Dana Goldstein, "'It Just Isn't Working': PISA Test Scores Cast Doubt on US Education Efforts," *New York Times*, December 3, 2019.

21. Todd Harrison, "The Air Force of the Future: A Comparison of Alternative Force Structures," Center for Strategic and International Studies, October 29, 2019.

22. Valerie Insinna, "Watchdog Group Finds F-35 Sustainment Costs Could Be Headed Off Affordability Cliff," *Defense News*, July 7, 2021; Sébastien Roblin, "The Air Force Admits the F-35 Fighter Jet Costs Too Much. So It Wants to Spend Even More," *NBC News*, March 7, 2021; Government Accountability Office, "F-35 Joint Strike Fighter: Cost Growth and Schedule Delays Continue," Report 22-105943, April 7, 2022; Aaron Gregg, "Powerful Lawmaker Calls F-35 Fighter Jet a 'Rathole,' Suggests Pentagon Should Cut Its Losses," *Washington Post*, March 5, 2021.

23. "US Defense Spending Compared to Other Countries," Peter G. Peterson Foundation, May 11, 2022; Anthony H. Cordesman, with the assistance of Grace Hwang, *Chinese Strategy and Military Forces in 2021: A Graphic Net Assessment*, revised August 3, 2021, 83–86; US Department of Defense, *Military and Security Developments Involving the People's Republic of China 2022: Annual Report to Congress,* November 29, 2022.

24. "Individuals Using the Internet," International Telecommunication Union (ITU), United Nations, 2022, https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx; Kelsey Campbell-Dollaghan, "Why One of World's Most Remote Places Has the Fastest Internet," *Gizmodo*, April 1, 2014; "Help with Internet and Social Media in an Authentic Bedouin Camp in Wadi Rum, Jordan," *Workaway.info*, updated January 2023, https://www.workaway.info/en/host/458895548546.

25. "Individuals Using the Internet."

26. Kai-Fu Lee, "Facial and Emotional Recognition; How One Man Is Advancing Artificial Intelligence," *60 Minutes*, interview by Scott Pelley, January 13, 2019.

27. James Vincent, "Putin Says the Nation That Leads AI 'Will Be the Ruler of the World,'" *The Verge*, September 4, 2017; Paul Mozur, "Beijing Wants AI to Be Made in China by 2030," *New York Times*, July 20, 2017.

28. Daniel R. Coats, "Worldwide Threat Assessment of the US Intelligence Community," Senate Select Committee on Intelligence, January 29, 2019, 17.

29. Alan Burkitt-Gray, "'Fourfold Increase' in Satellites over the Next 10 Years to 17,000," Capacity Media, December 10, 2021; The following section uses data from the Union of Concerned Scientists, which maintains one of the most comprehensive databases of active satellites. Data available at Union of Concerned Scientists, UCS Satellite Database, updated May 1, 2022, https://www.ucsusa.org/resources/satellite-database.

30. Union of Concerned Scientists, UCS Satellite Database.

31. Chris Gormeller, "Introducing 15 cm HD: The Highest Clarity from Commercial Satellite Imagery," Maxar Technologies, November 12, 2020.

32. Quoted in Philip Taubman, *Secret Empire: Eisenhower, the CIA, and the Hidden Story of America's Space Espionage* (New York: Simon & Schuster, 2003), 35.

33. Sami Quadri, "Former US Ambassador Says Russia Is Using 'Deepfakes to Impersonate Him,'" *Evening Standard*, October 1, 2022.

34. For greatest transfer of wealth, see Russell Flannery, "China Theft of US Information, IP One of Largest Wealth Transfers in History: FBI Chief," *Forbes*, July 7, 2020; for biggest long-term threat, see Christopher Wray, "Director's Remarks to Business Leaders in London," July 6, 2022, https://www.fbi.gov/news/speeches/directors-remarks-to-business-leaders-in-london-070622 (accessed March 10, 2023).

35. Lily Hay Newman, "It's Time to Get Real about TikTok's Risks," *Wired*, September 6, 2022.

36. Natasha Bertrand and Eric Wolff, "Nuclear Weapons Agency Breached amid Cyber Onslaught," *Politico*, December 17, 2020; Jon Porter, "White House Now Says 100 Companies Hit by SolarWinds Hack, but More May Be Impacted," *The Verge*, February 18, 2021; Dina Temple-Raston, "A 'Worst Nightmare' Cyberattack: The Untold Story of the SolarWinds Hack," *NPR*, April 17, 2021.

37. "Fake News Sets Off Twitter Confrontation between Pakistan and Israel," *CBS News*, December 25, 2016.

38. Chu Wang, "Twitter Diplomacy: Preventing Twitter Wars from Escalating to Real Wars," Belfer Center for Science and International Affairs, Harvard University, May 20, 2019; "Twitter Is the Prime Social Media Network for World Leaders," PR Newswire, May 31, 2017.

39. Jeff Jardins, "How Much Data Is Generated Each Day?" World Economic Forum, April 17, 2019.

40. Internet Live Stats, https://www.internetlivestats.com/one-second/#traffic-band (accessed December 7, 2022).

41. Tim Fisher, "Terabytes, Gigabytes, and Petabytes: How Big Are They?" *Lifewire*, January 1, 2021; Pranshu Verma, "This Chip Transmits an Internet's Worth of Data Every Second," *Washington Post*, October 27, 2022.

42. Cybersecurity Advisory, "Top CVEs Actively Exploited by People's Republic of China State-Sponsored Cyber Actors," white paper, October 6, 2022.

43. Stuart Lau, "China's Xi Warns Putin Not to Use Nuclear Arms in Ukraine," *Politico*, November 4, 2022.

44. Chris Buckley and Steven Lee Meyers, "In Beijing, Olympic Spectacle and Global Power Games," *New York Times*, February 4, 2022.

45. Eliot Higgins, "How Bellingcat Uncovered Russia's Secret Network of Assassins," *Wired*, April 2, 2021; Narjas Zatat, "Isis Supporters in Europe Are Accidentally Revealing Their Locations on Social Media," *Indy100*, May 22, 2016.

46. Will Croxton, "How Bellingcat Tracked a Russian Missile System in Ukraine," *60 Minutes Overtime*, February 23, 2020.

47. Jon Gambrell, "Analysts: Fire at Iran Nuclear Site Hit Centrifuge Facility," *Washington Post*, July 2, 2020.

48. Joby Warrick, "China Is Building More than 100 New Missile Silos in Its Western Desert, Analysts Say," *Washington Post*, June 30, 2021; Editorial Board, "More Missile Silos Have Been Found in China. That's an Ominous Sign," *Washington Post*, July 30, 2021.

49. Author interview, October 31, 2022.

50. Alexis C. Madrigal, "#BostonBombing: The Anatomy of a Misinformation Disaster," *The Atlantic*, April 19, 2013; Jay Caspian Kang, "Should Reddit Be Blamed for the Spreading of a Smear?" *New York Times*, July 25, 2013; Chris Wade, "The Reddit Reckoning," *Slate*, April 15, 2014.

51. Kelley M. Sayler, "Artificial Intelligence and National Security," Congressional Research Service Report R45178, November 10, 2020, 10.

52. Amy Zegart and Michael Morell, "Spies, Lies, and Algorithms: Why US Intelligence Must Adapt or Fail," *Foreign Affairs*, May/June 2019; "Maintaining the Intelligence Edge: A Report of the CSIS Technology and Intelligence Task Force," Center for Strategic and International Studies, January 2021; Elizabeth Leyne and Yvette Nonte, "Is the Intelligence Community Staying Ahead of the Digital Curve?" Harvard Belfer Center Report, August 2021.