Spies, Lies, and Algorithms

Why U.S. Intelligence Agencies Must Adapt or Fail

Amy Zegart and Michael Morell

For U.S. intelligence agencies, the twenty-first century began with a shock, when 19 al Qaeda operatives hijacked four planes and perpetrated the deadliest attack ever on U.S. soil. In the wake of the attack, the intelligence community mobilized with one overriding goal: preventing another 9/11. The CIA, the National Security Agency, and the 15 other components of the U.S. intelligence community restructured, reformed, and retooled. Congress appropriated billions of dollars to support the transformation.

That effort paid off. In the nearly two decades that U.S. intelligence agencies have been focused on fighting terrorists, they have foiled numerous plots to attack the U.S. homeland, tracked down Osama bin Laden, helped eliminate the Islamic State's caliphate, and found terrorists hiding everywhere from Afghan caves to Brussels apartment complexes. This has arguably been one of the most successful periods in the history of American intelligence.

But today, confronted with new threats that go well beyond terrorism, U.S. intelligence agencies face another moment of reckoning. From biotechnology and nanotechnology to quantum computing and artificial intelligence (AI), rapid technological change is giving U.S. adversaries new capabilities and eroding traditional U.S. intelligence advantages. The U.S. intelligence community must adapt to these shifts or risk failure as the nation's first line of defense.

Although U.S. intelligence agencies have taken initial steps in the right direction, they are not moving fast enough. In fact, the first intelligence breakdown of this new era has already come: the failure to

AMY ZEGART is a Senior Fellow at the Hoover Institution and at Stanford University's Freeman Spogli Institute for International Studies.

MICHAEL MORELL is former Deputy Director and Acting Director of the CIA. He is currently Global Chair of the Geopolitical Risk Practice at Beacon Global Strategies.

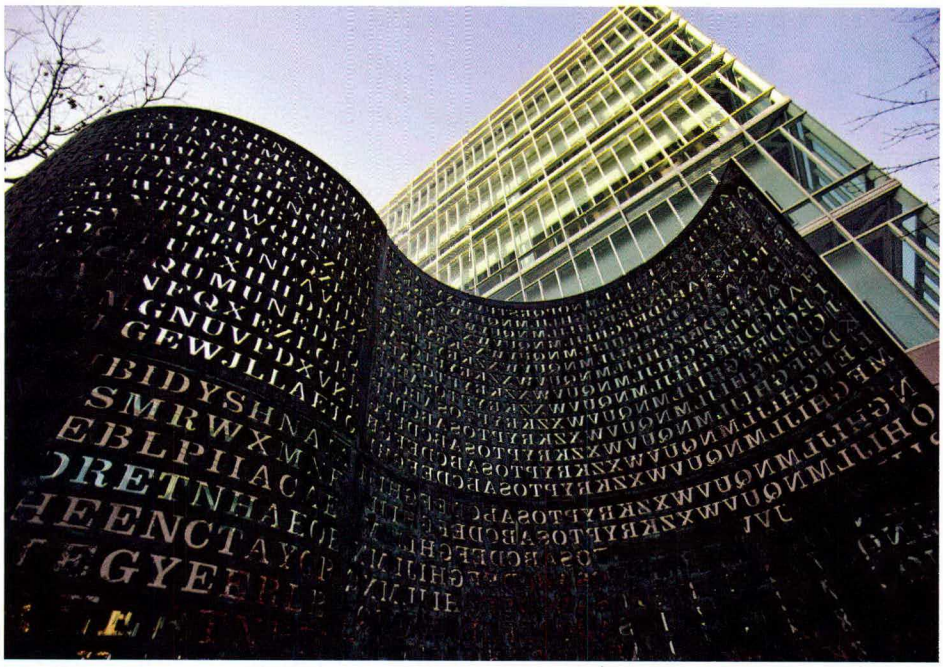
quickly identify and fully grasp the magnitude of Russia's use of social media to interfere in the 2016 U.S. presidential election. That breakdown should serve as a wake-up call. The trends it reflects warrant a wholesale reimagining of how the intelligence community operates. Getting there will require capitalizing on the United States' unique strengths, making tough organizational changes, and rebuilding trust with U.S. technology companies.

A WARNING SIGN

Russia's multifaceted "active measures" campaign ahead of the 2016 election was designed to undermine public faith in the U.S. democratic process, sow divisions in American society, and boost public support for one presidential candidate over another. Much of this effort did not go undetected for long. Almost immediately, U.S. intelligence agencies noticed Russian cyberattacks against the Democratic National Committee and Hillary Clinton's campaign, the sharing of stolen information with platforms such as WikiLeaks, and attempts to penetrate state and local voting systems. Pointing to these events, intelligence officials warned President Barack Obama well before the election that the United States was under attack.

Yet the intelligence agencies missed Russia's most important tool: the weaponization of social media. Studies commissioned by the Senate Intelligence Committee and Special Counsel Robert Mueller's indictment of a Russian "troll farm" show that the social media operation designed to undermine the U.S. electoral process may have begun as early as 2012 and was well under way by 2014. But although U.S. intelligence officials knew that Russia had used social media as a propaganda tool against its own citizens and its neighbors, particularly Ukraine, it took them at least two years to realize that similar efforts were being made in the United States. This lapse deprived the president of valuable time to fully understand Moscow's intentions and develop policy options before the election ever began.

In October 2016, one month before the election, James Clapper, the director of national intelligence, and Jeh Johnson, the secretary of homeland security, took the unusual step of issuing a public statement about Russia's interference in the election. Even then, the full extent of the Russian effort eluded U.S. intelligence; the statement did not mention social media at all. Johnson later stated that Russia's social media operation "was something . . . that we were just beginning to



Cracking the code: at CIA headquarters, Langley, Virginia, June 2010

see." Likewise, Clapper wrote in his memoir that "in the summer of 2015, it would never have occurred to us that low-level Russian intelligence operatives might be posing as Americans on social media." Indeed, the intelligence community did not understand the magnitude of the attack, which reached more than 120 million U.S. citizens, until well after the election. The Senate Intelligence Committee noted in 2018 that its own bipartisan investigation "exposed a far more extensive Russian effort to manipulate social media outlets to sow discord and to interfere in the 2016 election and American society" than the U.S. intelligence community had found even as late as 2017.

It was with good reason that the intelligence agencies did not have their collection systems trained on social media content within the United States, but Russia's social media attack was carried out by Russian nationals operating on Russian soil. They were assisted by several Russian intelligence operatives sent to the United States in 2014, with the express goal of studying how to make Moscow's social media campaign more effective. Whether the Kremlin tipped the balance in a close presidential race will never be known. What is clear, however, is that Russia's nefarious use of social media went undetected by U.S. intelligence for too long and that this failure is just a preview of what lies ahead if the intelligence community doesn't adapt to today's rapid technological breakthroughs.

DREW ANGERER / THE NEW YORK TIMES / REDUX

INDISPENSABLE INTEL

Intelligence has always been an essential part of warfare and statecraft. "Know the enemy," the Chinese military strategist Sun-tzu instructed around 500 BC. On the battlefield, good intelligence helps save lives and win wars by pinpointing hostile forces, anticipating their next moves, and understanding the adversary's intentions, plans, and capabilities. Off the battlefield, intelligence helps leaders make better decisions by preventing miscalculations and providing timely insights into threats and opportunities. In 1962, for example, intelligence collected by U-2 spy planes gave President John F. Kennedy the time and evidence he needed to compel the Soviet Union to remove nuclear weapons from Cuba without sparking a nuclear war. Of course, intelligence can also be wrong—sometimes disastrously so, as with assessments of Saddam Hussein's weapons of mass destruction programs before the Iraq war. Intelligence is, by nature, an uncertain business that involves piecing together fragments of information about adversaries who are intent on denial and deception.

But the enduring value of intelligence comes from a fundamental reality: government leaders make better decisions when they have better information. And U.S. intelligence agencies have long been able to deliver better information than other sources. Using both human agents and technical methods, they collect secret information that U.S. adversaries are trying to hide. They combine those secrets with data from other parts of the government and open-source information gleaned from news reports, unclassified foreign government documents, and public statements, to name but a few sources. They tailor their analysis to the specific needs of policymakers and deliver it without opinion, partisanship, or a policy agenda.

These capabilities are in high demand today. But new threats and new technologies are making intelligence collection and analysis far more challenging than at any time since the early days of the Cold War. Recent annual threat assessments from the Office of the Director of National Intelligence paint a head-spinning picture of global dangers: rising great-power competition, particularly from China and Russia; growing nuclear arsenals in North Korea and along the Indian-Pakistani border; a chaotic Middle East breeding extremism; an eroding international order; and autocrats on the march from Europe to Asia. Climate change is displacing thousands, compounding existing instability. Even fighting isn't what it used to be, with

"gray zone" conflicts and "little green men" blurring the line between war and peace.

At the same time, U.S. intelligence agencies are facing new challenges generated by breakthrough technologies. In 2007, the word "cyber" did not appear once in the annual intelligence threat assessment. In 2009, it was buried on page 38 of the 45-page document, just below a section on drug trafficking in West Africa. Yet by 2012, barely three years later, then Secretary of Defense Leon Panetta warned that a "cyber–Pearl Harbor" could devastate the United States' critical infrastructure without warning. Today, an assortment of malign actors perpetrate millions of cyberattacks around the world every day. Cybercrime now generates more revenue than the global illicit drug trade.

The combination of new technologies and the rising number, complexity, and velocity of threats means more danger for the United States—and greater demands on its intelligence agencies. Consider, for example, the emerging realm of U.S. offensive cyber-operations. In the physical world, many military targets are buildings that do not move, so target lists and operational plans have shelf lives. Planners can be sure that a bomb of sufficient yield will reduce to rubble any building in the blast radius, no matter how many windows it has or whether the walls are made of concrete or wood. Not so in cyberspace, where the targets are machines or systems that change constantly, in seconds. Even tiny modifications to a target (such as the installation of a simple patch) can render a cyberweapon against it completely useless, and the ever-shifting landscape makes it difficult to predict an attack's collateral damage. As a result, target lists require real-time updating to stay useful. In this world, intelligence is more than just a contributor. As Chris Inglis, former deputy director of the National Security Agency, recently wrote, intelligence is "an essential predicate" for effective action.

OPEN SECRETS

Advances in technology tend to be a double-edged sword for intelligence. Almost any technological development can make adversaries more capable and undermine existing defenses. At the same time, it can allow intelligence agencies to do their job better and faster. AI, for instance, can both improve analysis and make enemies' information warfare nearly impossible to detect. Commercial encryption services protect the communications of U.S. citizens and policymakers but

also enable terrorists to coordinate clandestinely. Technologies such as AI, facial recognition, and biometrics can help agencies catch wanted people, but they also make traditional clandestine operations difficult.

The explosion of open-source information—the result of connecting ever more smart devices to the Internet—offers perhaps the best unclassified example of the promise and perils of new technology. Over half of the world's population is now online. By some estimates, more people will have cell phones than access to running water next year. This connectivity is turning normal citizens into knowing or unwitting intelligence collectors. Cell phones can videotape events and even record seismic activities, such as underground nuclear tests, in real time. Surveillance cameras capture much of what takes place in cities around the world. Social media, search engines, and online retail platforms expose a great deal of information about users. For analysts, this is a treasure-trove of information. Secrets still matter, but open-source information is becoming more ubiquitous and potentially valuable—both to the United States and to its adversaries.

Open-source information offers access to areas that secret sources can have a hard time penetrating.

Open-source information even offers access to areas that secret sources can have a hard time penetrating. When Russia invaded eastern Ukraine in 2014, the most compelling evidence came from time-stamped photos taken by Russian soldiers and posted on social media, showing tank transporters and Ukrainian highway signs in the background. Likewise, social media captured how Russia's sophisticated SA-11 air defense system was moved into eastern Ukraine just before the shootdown of Malaysia Airlines Flight 17 and later transported back to Russia. Social media has become such a valuable resource that consoles at U.S. Strategic Command's underground nuclear command center now display Twitter alongside classified information feeds.

At the same time, easy access to data and technologies is leveling the intelligence playing field at the United States' expense. More countries, including U.S. adversaries such as Iran and North Korea, as well as nonstate actors, can now collect intelligence worldwide at little cost. Anyone with an Internet connection can see images on Google Maps, track events on Twitter, and mine the Web with facial recognition software. When U.S. Navy SEALs raided bin Laden's

compound in Pakistan in 2011, the Pakistani military did not detect the operation—but a local information technology consultant named Sohaib Athar did. As U.S. forces were landing, Athar started tweeting about hearing unusual noises. "Helicopter hovering above Abbottabad at 1AM (is a rare event)," he wrote. Athar continued unwittingly live-tweeting the raid, even reporting that an explosion shook his windows. It is easy to imagine how similar incidents could put future U.S. operations at risk.

Commercial satellites, meanwhile, now offer low-cost eyes in the sky for anyone who wants them. Until about a decade ago, the United States and Russia dominated the space market with a handful of large spy satellites that were each the size of a bus, cost billions apiece to design and launch, used highly advanced technology, and produced classified information. China has now joined that elite group. But plummeting launch costs, enhanced commercial optics, and miniaturization are spreading space technology even further. In the past five years, the number of countries owning and operating satellites has doubled, and the annual number of launches has increased by 400 percent. In December 2018, the aerospace company SpaceX launched a rocket containing 64 small satellites from 17 countries. Inexpensive satellites roughly the size of a shoebox offer imagery and analysis to paying customers worldwide. Although no match for U.S. government capabilities, these satellites are getting better day by day.

THE DECEPTION REVOLUTION

The U.S. intelligence community must figure out how to harness the open-source revolution and an array of other technologies faster and better than American adversaries. At the same time, it must balance this effort with its constitutional and ethical obligations to safeguard privacy and civil liberties.

This is easier said than done. Consider, once again, the case of open-source data. In the Middle Ages, when paper was a sign of wealth and books were locked up in monasteries, knowledge was valuable and creating it was costly. Now, creating content is so cheap that, by some estimates, the amount of data stored on earth doubles every two years, meaning that humankind will produce as much data in the next 24 months as it has throughout its entire history so far. Intelligence agencies have always had to find needles in haystacks. Today, the haystacks are growing exponentially.

A large number of private-sector companies are delivering "social listening" and other solutions that take advantage of open-source information and are able to quickly assess it. The CIA-affiliated venture-capital firm In-Q-Tel has nurtured many promising technology start-ups with seed money. But getting any technological innovations to take root inside the intelligence agencies has been a challenge, thanks to embedded contractors with their own financial incentives, bespoke and aging information technology systems, and sclerotic, risk-averse acquisition policies that make it exceptionally difficult for commercial companies, especially start-ups, to work with the government.

To stay relevant, intelligence analysts are forced to move faster—sometimes at the expense of digging deeper.

Collecting and processing all the data is only half the battle. More information is of little use unless analysts can assess what information is credible and what isn't. Credibility, enough of a challenge when it comes to secret intelligence, is an even bigger problem in the open-source world. Bloggers, citizen reporters, and other online content providers operate with different incentives that put a premium on being quick and provocative rather than correct and rigorous. As a result, the risk of error is significant.

Add to this the growing challenge of timeliness. In the era of Google, when information from anyone about anything is just a swipe or a click away, open-source content increasingly flows right into the hands of policymakers without vetting or analysis. This raises the risk that policymakers will make premature judgments instead of waiting for slower-moving intelligence assessments that carefully consider source credibility and offer alternative interpretations of breaking developments. To stay relevant in this environment, intelligence analysts are forced to move faster—sometimes at the expense of digging deeper. Competition with open sources also may exacerbate pressures for analysts to produce short-term intelligence assessments rather than longer-term, over-the-horizon analysis, something that is already in short supply.

Separating the true from the spurious will only become more difficult. AI is giving rise to a deception revolution. Russian disinformation ahead of the 2016 election pales in comparison to what will soon be possible with the help of deepfakes—digitally manipulated audio

or video material designed to be as realistic as possible. Already, commercial and academic researchers have created remarkably lifelike photographs of nonexistent people. Teams at Stanford University and the University of Washington have each used AI and lip-synching technology to generate deepfake videos of Barack Obama saying sentences he never actually uttered. As with other technologies, access to simplified deepfake code is spreading rapidly. Some programs are easy enough that high schoolers with no background in computer science can use them to generate convincing forgeries. Even the high-end computing power needed for more sophisticated deepfakes can now be acquired at relatively low cost.

It does not take much to realize the manipulative potential of this technology. Imagine watching a seemingly real video that depicts a foreign leader discussing plans to build a clandestine nuclear weapons program or a presidential candidate molesting a child just days before an election. Their denials could easily be dismissed because the evidence seems incontrovertible—after all, seeing has always been believing.

Intelligence agencies will face the Herculean task of exposing deepfakes. And unlike other forgeries, such as doctored images, deepfakes are uniquely hard to detect, thanks to an AI technique invented by a Google engineer in 2014. Known as "generative adversarial networks," the approach pits two computer algorithms against each other, one generating images while the other attempts to spot fakes. Because the algorithms learn by competing with each other, any deepfake detectors are unlikely to work for long before being outsmarted. Deception has always been part of espionage and warfare, but not with this level of precision, reach, and speed.

GETTING THE STRATEGY RIGHT

The U.S. intelligence community has taken some important steps to adapt to this rapidly changing technological landscape. In 2015, then CIA Director John Brennan created a new directorate focused on digital innovation and overhauled the CIA's structure, in part to bring digital specialists and open-source intelligence officers closer together with the CIA's traditional collectors and analysts. The National Geospatial-Intelligence Agency has started an AI initiative to accelerate and improve imagery analysis. The CIA, the National Security Agency, and other agencies have moved to the cloud, creating a "big-data fusion environ-

ment" that enables analysts to query large quantities of data faster and more effectively. Many other improvements remain classified.

These are promising efforts, but individual fixes are not enough. The intelligence community needs a comprehensive strategy to regain and sustain the nation's intelligence advantage in a new technological era. The 2019 National Intelligence Strategy falls far short of this goal, striking a decidedly complacent tone and containing vague exhortations to "increase integration and coordination," "better leverage partnerships," and "increase transparency while protecting national security information." Innovation is relegated to just half a page.

A national intelligence strategy for the new technology age should begin by identifying the United States' distinctive strengths and how they can be used to secure long-term advantage. Much of today's foreign policy discussion focuses on the United States' weaknesses, painting a picture of a nation that is isolated, vulnerable, and outmatched by ruthless and efficient autocrats. A new intelligence strategy should flip the script. Rather than succumbing to authoritarian envy, the starting point should be recognizing what the United States has that none of its competitors can match and how these capabilities can compensate for any vulnerabilities.

The United States surpasses its adversaries on a number of fronts. A broad array of alliances—including the Five Eyes intelligence partnership, with Australia, Canada, New Zealand, and the United Kingdom—extends the United States' global reach and capabilities. An ethnically diverse population offers a natural edge in collecting human intelligence around the world. The United States' open society and democratic values have long encouraged the free flow of ideas and helped persuade foreign nations and individuals to join its cause. And the United States' innovation ecosystem continues to serve as an unrivaled incubator of breakthrough technologies.

Leveraging these strengths, however, will require a broad-based, intelligence-community-wide effort with input from technology companies, civil society, and academia. A blue-ribbon commission, instituted and overseen by Congress, could drive this change. It is impossible to predict what insights and initiatives this process would yield, but several areas of focus are already apparent.

On the organizational front, open-source intelligence deserves its own agency. Currently, its collection runs through the CIA's Open Source Enterprise, but this setup is akin to keeping the air force within

the army, hobbling a new mission by putting it inside a bureaucracy that naturally favors other priorities. Secrets still reign supreme in the CIA, relegating open-source information to second-class status. Open-source intelligence will never get the focus and funding it requires as long as it sits inside the CIA or any other existing agency.

Human capital will be just as essential. The current employment system in the intelligence agencies was designed for a different time, when intelligence officers spent their entire careers in the government. Today, at some agencies, many first-rate employees walk out the door after just a few years, taking their expertise and training with them, never to return. Many more never even walk in, owing to a slow and bureaucratic recruitment process. Technological expertise is particularly hard to attract and retain. And the intelligence agencies need to create more ambassadors, not just lifers—bringing young and midcareer technologists in and out of the government to improve relationships, understanding, and trust between the U.S. technology industry and the intelligence community.

Indeed, bridging the divide between the technology industry and the intelligence community is a national security imperative. For major technology companies such as Apple, Facebook, Google, and others, the surveillance programs revealed by the former defense contractor Edward Snowden in 2013 created a deep and abiding trust deficit. Twitter won't do business with intelligence agencies out of concerns about how its information will be used. A senior executive at a major technology company and a former senior executive at another leading technology firm told one of the authors that they consider U.S. intelligence agencies adversaries that, similar to Chinese government operatives, must be kept out of their systems.

The intelligence community, for its part, is more and more concerned about the willingness of U.S. technology companies to sell their products and services to foreign clients who do not share the United States' democratic principles or national interests. Google, which has some of the most sophisticated AI capabilities in the world, has said that it will not work with the Pentagon on any AI projects that could be used in making weapons, but it is considering helping the Chinese government develop a better-censored search engine. Russia's highly touted deep-learning project iPavlov uses hardware from NVIDIA, a cutting-edge California-based chip company. "We sell those to everyone," NVIDIA's vice president for business development recently said publicly. Managing this clash of commercial incentives,

privacy, and national interests requires a better working relationship between the U.S. intelligence community and Silicon Valley.

FIRST PRINCIPLES

For all that needs to change, even more important is what should not. The first priority of any transformation effort should be to do no harm to the intelligence community's most valuable asset: its commitment to objectivity, no matter the policy or political consequences. This principle explains why generations of policymakers have trusted the intelligence community's work—not trust in the sense that the intelligence is always correct (it is not) but trust in the sense that there is no ulterior motive, policy agenda, or partisan view driving it.

This core principle is being tested by a president who publicly disparages his intelligence officers and disagrees openly with their agencies' assessments. Such behavior puts pressure on the intelligence community to "call it" the president's way rather than going where the evidence leads. So far, under Director of National Intelligence Dan Coats, the intelligence community is holding firm to its ethos. But the risks are high. The U.S. intelligence community can develop the best strategy for intelligence in a new technological era, but if it ever loses its reputation for objectivity, nonpartisanship, and professionalism, it will lose its value to the nation.