The Declining Market for Secrets
U.S. Spy Agencies Must Adapt to an Open-Source World

BY ZACHERY TYSON BROWN AND CARMEN A. MEDINA
March 9, 2021

For nearly three-quarters of a century, the United States intelligence community has supplied American military and political leaders with information and analysis intended to help them make better decisions about critical national security concerns. During the Cold War—when the United States and the Soviet Union went to extraordinary lengths to reveal as little as possible about themselves and learn as much as possible about each other—the most valuable information was inevitably secret information. The spy planes, listening posts, and other “sources and methods” that were contrived to extract this information were expensive to develop and maintain, and the
elaborate security architecture that evolved to protect them endures to this day.

Since the end of the Cold War, however, that closed intelligence architecture has increasingly become an impediment to the timely communication of information. In an era of abundant data, rapid change, and novel threats to American interests, the frictionless communication of ideas and facts is arguably more important than protecting the tools used to gather them. Today’s national security leaders—inundated with potentially useful information yet compelled to work within a system that restricts its flow—are often driven to seek more convenient sources elsewhere.

While the agencies that make up the U.S. intelligence community were built to dominate a world of secrets, we believe their future success will depend on their ability to effectively operate out in the open. One of us (Carmen Medina) began raising concerns about the intelligence community’s traditional model nearly 20 years ago. The other (Zachery Tyson Brown) researched related topics at National Intelligence University in 2017. Although separated by generation, agency, and seniority, we had independently identified the same persistent problems and had begun thinking along similar lines about how to solve them.

Of course, we were hardly the first to recognize that Washington’s intelligence agencies would need to reinvent themselves in order to remain relevant. The history of American intelligence reform is as long as it is frustrating. The former Director of Central Intelligence Stansfield Turner, convinced that the greatest future threats to the United States would arise not from armed conflict but from political and economic instability, once argued in these pages that intelligence analysis must make better use of open sources and must become more interdisciplinary. Although this insight
is one today’s intelligence community is just beginning to recognize, Turner’s advice was written 30 years ago.

In recent months, calls to revitalize American intelligence have intensified. Most of the accompanying policy proposals, however, have remained fairly conventional—focused on reversing perceived politicization, for example, or on adopting new technologies. These measures are insufficient, we believe, because they leave the closed machinery of intelligence collection and dissemination untouched. Although this enormous global apparatus produces an estimated 50,000 intelligence reports per year, security standards are so strict that many of them are read only by other intelligence officers. Despite its mission to “speak truth to power,” the intelligence community is often talking only to itself.

A NEW ECOSYSTEM

The information revolution has seeded a growing ecosystem of open-source intelligence services. Firms such as Recorded Future, DigitalGlobe, and McKinsey offer not only intelligence-like products, such as news aggregation and data analytics, but also such services as on-demand overhead satellite imagery and long-term strategic forecasting that were previously the purview of governments alone. Some organizations, such as Bellingcat, have blurred the line between journalism and intelligence by pioneering open-source techniques that exploit social media, commercial imagery, and gray literature.

Private firms and journalistic outfits now often beat the intelligence community at its own game—at least in terms of speed and accessibility. And while intelligence community leaders might comfort themselves by pointing out that outsiders’ techniques aren’t as sophisticated or authoritative as their own, the truth is that speed and accessibility win every
time (a retired senior CIA operations officer recently acknowledged as much on Twitter, noting that the CIA must adapt or risk irrelevance).

Nonetheless, the intelligence community still works under a flawed assumption of exclusivity. Agencies require users to be in secure facilities just to access intelligence the community creates, and the system, which spends the bulk of its budget on expensive collection methods, expects analysts to justify the expense by maximizing the amount of highly classified material in their papers and presentations. Analysts have little, if any, incentive to make their product more accessible. But the emphasis on secretly collected information is usually unnecessary: the same or similar information that was gathered through secret means can often be found in open sources that require no security protections and that intelligence officers might fruitfully explore if they were not discouraged from doing so. To reverse this isolating trend, open-source information and open-access research and analysis techniques must become a routine part of intelligence work—the foundation, not the exception.

**THINKING OUTSIDE THE BIN**

The United States now finds itself in the throes of both a deadly pandemic and a disinformation campaign that has driven political unrest. Accordingly, Washington must broaden its conception of national security to include more than the obvious threats posed by foreign militaries and terrorist networks. Overlapping webs of influence and power run over, under, and through governments, political parties, and individuals. Domestic and foreign threats frequently shade into one another, and local governments, private enterprise, and individual citizens easily find themselves on the frontlines of great-power competition. What cybersecurity experts call the “attack surface” stretches across the entire planet, rendering distance irrelevant and opening the nation to manipulation or even attack by almost
anyone from almost anywhere. The battles that take place within this so-called information space may be virtual, but their consequences—from self-radicalization to the hijacking of critical infrastructure—are real.

The intelligence community’s traditional frameworks are remarkably unsuited for this new era of ubiquitous connectivity. Policymakers—and even many intelligence officers—are trained to approach national security as a collection of discrete issues that can be neatly placed into bins. Ballistic missiles over here, for example; climate change over there. Having bins for every conceivable problem helps the government to divvy up budgets and personnel—but today the problems in every bin can interact with all the others and produce results that such separation makes harder to predict. A closed intelligence community isolates each bin of concerns from all the others by erecting walls of secrecy around the production and analysis of intelligence within a given subject area. Erected in the beginning to protect sensitive sources and methods, these walls have today grown so tall that we believe they are doing more harm than good.

An open intelligence community would instead recognize that threats to national security can emerge spontaneously and unexpectedly from vectors that were once considered relatively harmless. It would focus less on analysis than on synthesis—on understanding problems not discretely but as an integrated whole. Such holistic thinking would not only produce more ideas and better solutions; it would also provide policymakers with a more comprehensive understanding of the multifaceted issues their policies must address.

TIME IS OF THE ESSENCE
A senior CIA official noted a decade ago that policymakers’ most precious commodity is time. And few have enough of that priceless resource to spend hours or days tracking down and consuming intelligence. At present, only the handful of officials who receive the President’s Daily Brief are offered intelligence in a convenient format, at the time and place of their choosing, no matter where in the world they may be. And even those select few can often spare only a fleeting glance at the brief’s contents.

The rest of the national security workforce includes officials across the defense, law enforcement, and policymaking communities who frame discussions and make decisions every day. And most of them can access intelligence only behind heavy vault doors, often in a building’s basement or an hour’s drive across town. Those whose days are measured in back-to-back meetings and by inboxes full of unread emails have little time or incentive to seek out highly classified intelligence.

Open-source providers, by contrast, are eager to facilitate access to their services. User experience is the standard by which they succeed or fail. The intelligence community has to be able to do the same. Today, the National Geospatial-Intelligence Agency is the only intelligence community component with a presence on the Google Play and Apple app stores. Why is this agency so far ahead? Because it realized years ago as commercial imagery companies exploded on the scene that it would not long survive as a primarily secret organization.

The rest of the intelligence community is overdue for the same wake-up call. Today’s users of intelligence quite simply expect more—more transparency as a matter of course but also more convenience and more collaboration between what we once simplistically called “producers” and “consumers.” National security professionals across government should be
able to access intelligence swiftly, easily, and in a manner that better facilitates both their routine work and the crucial decisions they make.

**A NEW MEDIUM**

The closed architecture of the intelligence community was not built in a day or even a decade. A more open future likewise will not materialize overnight. Rather, the very way Americans conceive of intelligence must evolve through experimentation and recalibration that protects the intelligence community’s foundations while encouraging new growth.

We begin with a modest proposal. Imagine a dynamic content platform, authorized by the director of national intelligence, that users could access from any location and on any device. This platform would supply intelligence in an easy, distinctive, and user-friendly format to anyone who works in national security. The information would be protected by a virtual private network, and at first, while the community gained experience with the new system, only less-sensitive material would be allowed on the platform.

At the outset, intelligence officers would be encouraged but not required to create and post content. They might, for example, offer new analytic lines of thought, highlighting curious new perspectives from diverse sources. They might simply post idle musings that could then catch the interest of other analysts they otherwise would have never encountered. Moderators would ensure that the atmosphere remained professional and grounded in reality. Any authorized user of the platform could comment openly and choose to receive encrypted text messages summarizing new content.

Such a platform would allow intelligence analysts to supply context and
immediate feedback when news broke. Users would be able to experiment with new formats and approaches: for example, analysts and policymakers could collaborate in threaded discussions to evaluate new developments. By interacting with one another and observing different approaches to analysis and synthesis, analysts could stimulate each other’s creativity—a quality often said to be lacking in the craft of intelligence. Some adaptations will prove successful; others will be discarded. But the platform would evolve and grow much like other modern technologies have—that is, in ways the designers might not have anticipated but that reflect the needs of users.

The U.S. intelligence community should not stop collecting and keeping secrets altogether. Intelligence professionals will always remain in the business of finding out what foreign leaders are saying behind closed doors, for example, or assessing an enemy before a battlefield encounter. But the United States should place less emphasis on hard intelligence and realign its limited resources accordingly. As intelligence users become satisfied with the insight and context that a more open platform can provide, collection managers will be able to shift their focus, concentrating on those really difficult problems that only exquisite intelligence collection capabilities can address.