BRUCE BERKOWITZ

The R&D Future of Intelligence

The U.S. intelligence community faces a changing landscape. Here is a blueprint for how it can best harness the potential of technology. One key: foster risk-taking.

The United States has long depended on its capability to develop and use technology for collecting and analyzing intelligence in order to protect national security. Indeed, the intelligence community has a remarkable record in R&D. Among its achievements, it has pioneered digital computers; a host of advanced aircraft, such as the high-altitude U-2 and its Mach 3 successor, the A-12; some of the earliest satellites; electro-optical sensors and the processing systems to support them; and, more recently, robotics.

But is U.S. intelligence prepared to use technology effectively in the future? The short answer is, "yes, but." The intelligence community faces two challenges.

First, threats to the United States are changing, and so intelligence targets are changing. In addition to traditional military competitors and rogue states, the United States now must also worry more about weapons of mass destruction (WMD) and transnational terror networks. Collecting and analyzing intelligence about many of these new targets requires new approaches and therefore new technologies.

Second, the world of technology is itself changing. When the intelligence community was established, most R&D took place in the United States, and the federal government funded most of that. Today, the opposite is true: Most R&D is taking place overseas; and even within the United States, most of it is funded by commercial and other nongovernment organizations.

These two developments—changes in the threat and changes in the world of R&D—define the two most important factors U.S. intelligence must deal with to keep its technology edge.

Landscape of intelligence

To better understand the problems that R&D for intelligence faces, it first helps to consider the topic of intelligence technology from several perspectives. One can think about the kinds of technology that intelligence organizations

Cesar Hidalgo

Cesar Hidalgo, a native of Santiago, Chile, and now a researcher at the Center for Complex Network Research at the University of Notre Dame, writes, "One of the most well-known clichés is that everything is connected. Unfortunately, this does not get at the most interesting question: It is not if we are connected, but how." Hidalgo's artwork explores ways to visualize data that are aesthetically appealing so that the viewer is encouraged to contemplate the image and consider the significance of the patterns of interaction. The visualizations reproduced here represent data on medical records, international trade, and mobile phone communications. All of them are spin-offs of figures produced for scientific publications.

Images courtesy of the artist.

use, the kinds of intelligence these technical systems produce, and the organizations that are responsible for developing intelligence technology and operating technical intelligence systems.

Most intelligence technologies fit into four basic categories:

• Sensors—optical, electronic, chemical, acoustic, nuclear, seismic, and geospatial—that collect data.

• Platforms—manned or robotic aircraft, ships, submarines, and satellites—that carry sensors where they need to be.

• Computers, networks, and software that process, compile, collate, and deliver data and finished intelligence.

• Enabling devices—covert communications, miniaturized cameras, hidden containers, and lock-picking tools—that make traditional espionage operations possible.

In general, the technologies that the intelligence community uses are not that much different from what is understood in the outside world, and the intelligence community depends more than ever on the R&D base that everyone else draws from. The differences lie in their specialized features and how quickly they are delivered into operation relative to the usual pace of technology development.

Intelligence technology also can be broken down into what specialists call INTs, or intelligence disciplines. This categorization is useful because each discipline entails different training, culture, and, sometimes, technology; much like medical specialties or engineering, which can be mechanical, chemical, or electrical. These intelligence disciplines include:

• Signals intelligence (SIGINT), which includes intercepts, and often decryption, of electronic communications. These modes of communication can be spoken word, text, or facsimile but also can include telemetry from missile or aircraft tests or even mechanical control data.

• Imagery intelligence (IMINT), which includes literal photographic, digital, or radar pictures of targets.

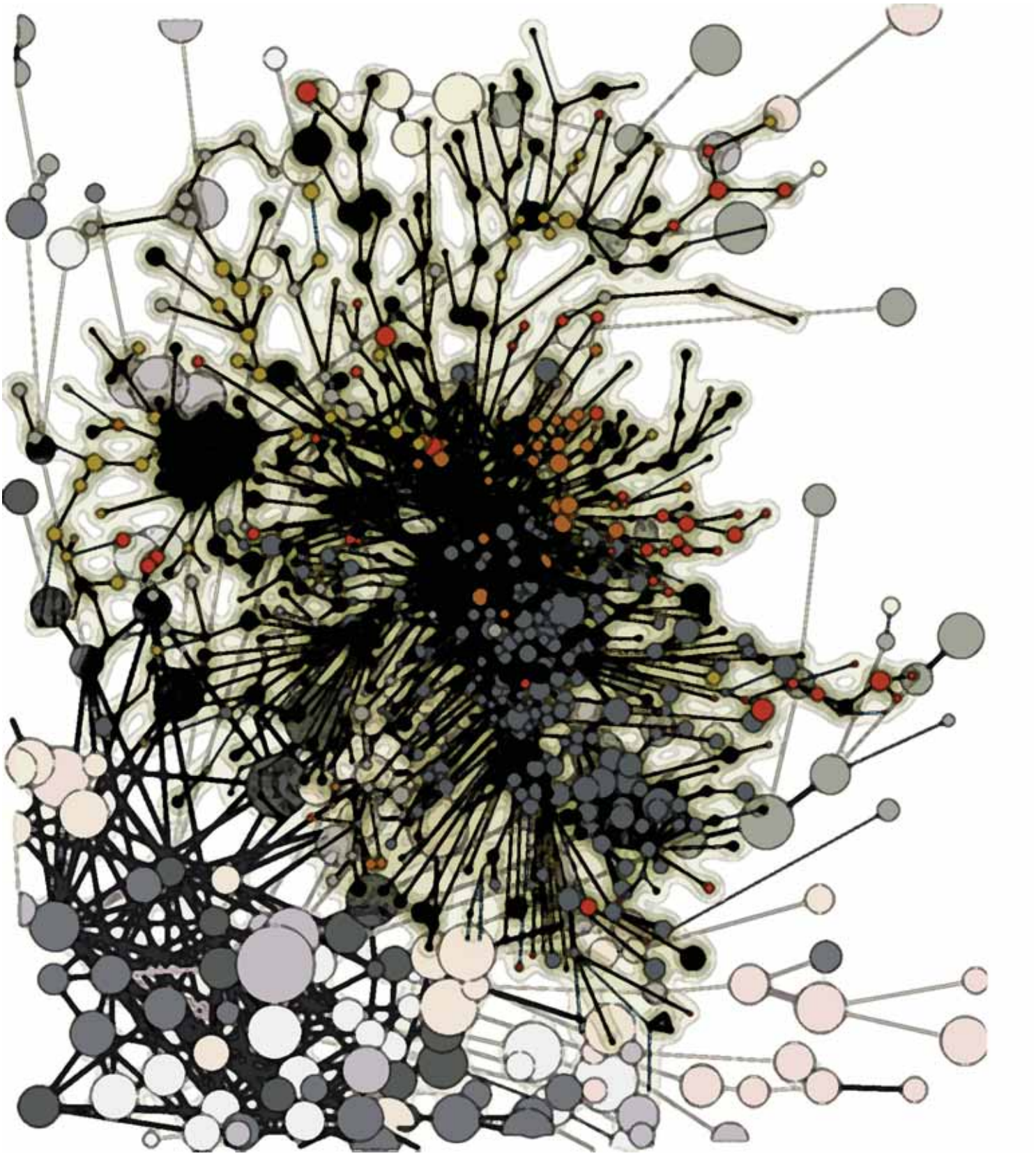
• Geospatial intelligence (GEOINT), which is the information derived by analyzing, manipulating, and combining such data, usually digitally, and often in reference to their position relative to each other or Earth's surface.

• Measurement and signatures intelligence (MASINT), which includes nuclear, acoustic, or spectral data used to detect the presence or characteristics of a target.

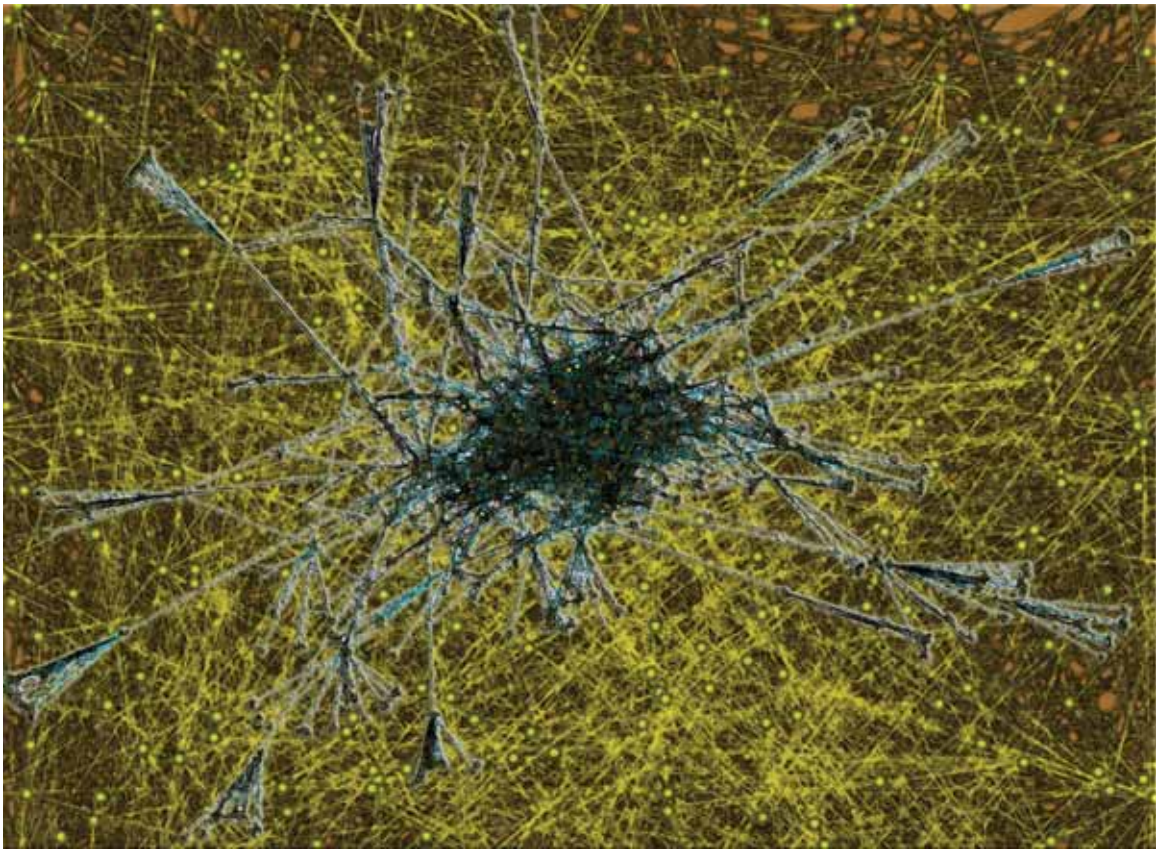
Besides these technical INTs, intelligence collected by human beings (called, logically enough, HUMINT) also remains important. Indeed, because intelligence technology and HUMINT are so often dependent on each other today, it is hard to discuss one without referring to the other.

Lately, intelligence specialists also have begun to refer something called OSINT, for open source technology intelligence. This grouping, which includes public media and databases, can be collected either through technology (for example, listening to foreign language broadcasts) or by humans (for example, by personally analyzing unclassified reports from scholars and journalists).

Another way to think about intelligence technologies is by the organizations responsible for them. This categorization is important because it is these organizations that recruit and train people, manage existing programs, and pro-



CESAR HIDALGO, *Black Forest*, Nodes are products, and links connect products likely to be exported by the same country, 2007.



CESAR HIDALGO, *Crowd*, Map of mobile phone calls during one year, 2008.

pose new ones. The big five are:

• The National Security Agency, which is responsible for most signals intelligence.

• The National Reconnaissance Office, which builds and operates most intelligence satellites.

• The National Geospatial Intelligence Agency, which is responsible for imagery databases and processing systems.

• The various technical military intelligence programs that operate under the direction of the Defense Intelligence Agency; these programs include seaborne and airborne platforms that the military services operate and certain measurement and signatures intelligence systems, such as large radar and sonar systems.

• The Central Intelligence Agency, which has been involved in all of these technologies, especially when they have involved traditional espionage or required funding outside of normal channels.

In addition, the Department of Energy develops technologies related to collecting intelligence about nuclear weapons. This activity, based primarily at national laboratories, is much smaller in terms of people and dollars than the Big Five activities but is obviously important. Also, most agencies with analytic functions are responsible for the technologies they use to manage databases and to assist analysts in handling and presenting information.

Technology is thus woven throughout the intelligence community, and several agencies owe their existence to the importance of particular kinds of technology. Even so, up to now no organization has had R&D as its main responsibility. Also, no organization has had as its primary responsibility ensuring that these technologies work together effectively.

This lack has sometimes caused problems. When embedded in operating organizations, R&D must compete directly with current programs for funds. Officials have only so much time and political capital, and it can take as much effort to defend a $5 million R&D project as a $5 billion acquisition program. R&D can thus get lost in the tussle of day-to-day planning and politics.

Also, because the organizations that operate systems have been the very ones responsible for developing the technology these systems use, the intelligence community has sometimes missed opportunities in which two or more technologies might work well in combination; for example, detecting the presence of radar in a region with signals intelligence and then pinpointing its exact location with imagery intelligence.

To be sure, intelligence organizations do collaborate (Allied forces used SIGINT to cue IMINT even in World War II), but without someone responsible for championing collaboration, R&D on multi-intelligence approaches is not the norm. Each organization has usually focused on how to solve an intelligence problem with its own technology, rather than considering collaboration at the beginning of the R&D process, when the latitude for defining a collection concept is greatest.

Most intelligence experts and legislators who oversee the intelligence community understand these issues. This was one reason why Congress in its 2004 intelligence reform legislation created a director of science and technology to be responsible for developing a "long-term strategy for scientific advances in the field of intelligence." Such awareness also probably led President Bush's Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction to recommend in 2005 that the intelligence community create "an authority responsible for managing and overseeing innovative technologies." This later emerged as the Intelligence Advanced Research Project Activity (IARPA), announced in 2006 and formally established in 2007.

IARPA was intended in the same spirit as the Defense Advanced Research Projects Agency (DARPA), which had been created in 1962. Most experts seem to agree that DARPA is a success. It has delivered technology that has transformed U.S. military operations. It can claim much of the credit for the Internet, the Global Positioning System, and the stealth technology that makes aircraft and other objects nearly invisible to radar, sonar, or other similar detection systems. The hope among officials is that IARPA will prove similarly successful.

However, simply replicating DARPA will not be enough. Because intelligence organizations have special challenges in dealing with the changing threats and the changing R&D environment, a new model is needed.

Moving intelligence targets

Today's intelligence community and the technology it uses were originally designed mainly to watch the Soviet Union. The chief concerns during the Cold War were a strategic nuclear attack against the United States or a military invasion of Western Europe. So the main intelligence targets were the Soviet Union's nuclear forces, its mechanized armies, the massive industrial complex that produced these weapons, and the highly centralized government that controlled them all.

These targets happened to lend themselves to technical observation. Soviet bomber bases and missile silos, for example, were big immobile objects that could be readily counted and analyzed with overhead imagery, as were the Soviet Union's mechanized army units and defense industries. So once one solved the problem of building an aircraft such as the U-2 or a satellite such as CORONA to collect the imagery, solving the intelligence problem was straightforward.

Other conditions peculiar to the Soviet target also facilitated a technological solution to intelligence problems. For example, because the Soviet landmass was so vast and difficult to traverse, Soviet leaders relied on long-distance radio links and marine cables laid around its coasts to communicate with outlying regions. These constraints funneled Soviet communications into a manageable number of channels that U.S. intelligence could tap. Favorable geography also made it possible to intercept telemetry from Soviet missile tests.

By the 1980s, though, strategic weapons were becoming smaller and more mobile. Better information technology enabled the Soviets to encrypt their communications and telemetry more easily and more effectively. It was inevitable that technical intelligence collection would become harder, and these limitations might have become apparent sooner had it not been for arms control. The SALT, START, and INF agreements all contained provisions specifically intended to enable each county's intelligence services to count its opponent's weapons with "national technical means"—a treaty term invented to refer to signals intelligence and imagery intelligence. Both superpowers accepted these measures because they wanted an arms control agreement.

In reality, the way U-2 imagery quickly dispelled the bomber gap of the 1950s and CORONA imagery dispelled the missile gap of the 1960s and 1970s were special cases. Weapons are rarely as easy to count as were bombers or missile silos during those earlier periods. The use of technologies comprising national technical means to monitor arms control (in effect, where one country helps another country to spy on it) was even more unusual. Usually adversaries do whatever they can to confound their opponent's intelligence.

Today, the world is returning to the historical norm in the relationship between hunting and hiding intelligence targets, where technical intelligence (like most intelligence) is often useful, but there are few significant intelligence prob-

lems that can be solved decisively and reliably by single intelligence disciplines. The targets of greatest concern—small dispersed terrorist cells and clandestine programs to develop WMD—are inherently difficult to monitor through any means, technical or otherwise. A technological silver bullet is unlikely. Technical intelligence collection will more probably provide only fragments of information. Some fragments may prove very important, but most will be incomplete and filled with uncertainty.

For example, consider a list of national security missions that the intelligence community must support today. It would probably include detecting hidden facilities for manufacturing nuclear, chemical, or biological weapons; identifying clandestine transnational terrorist networks; assessing foreign military forces, often designed for operations different from those planned by U.S. forces; analyzing international criminal trafficking; and maintaining border security against foreign intruders.

In every case, it is easy to think of how technical intelligence might be useful but hard to think of how any of these problems might be solved by a single technology or by technology alone. These are all complex requirements, calling for the use of several technical collection systems in combination, as well as analytic support to target the collection and assemble data, and perhaps support from human intelligence, to gain access. For example, if a foreign military or terrorist organization used a cellular communication system, an IMINT analyst could locate the node most vulnerable to attack, a HUMINT case officer could recruit someone with access to the system, and a SIGINT technical expert could design a bug tailored for the specific network.

R&D for the technology part of this kind of combined effort requires scientists and engineers to work more closely than ever with intelligence operators and analysts. More important, whereas in the past organizations might collaborate with personnel and technologies that they had already developed, in the future it will be more important to collaborate when the technology is being selected, designed, and developed. Establishing a venue in which all these specialists can work together at an early stage is vital.

Challenges of globalization

Funding for R&D in the United States has grown almost 10-fold during the five decades in which the National Science Foundation has published statistics. Adjusting for inflation and using today's dollars, total annual funding for R&D rose from about $35 billion in 1953 to about $310 billion in 2006.

This is impressive growth, but changes in the composition of R&D funding are even more significant. In 1953, the government provided 55% of all funding for R&D in the United States. During the 1960s, government funding accounted for up to two-thirds of all R&D, reflecting the space race and the Vietnam-era military buildup. The distribution returned to a near-even split between government and the private sector in the 1980s. Then commercial R&D funding began a period of remarkable growth, so that today nongovernment organizations provide 65 to 70% of all U.S. R&D funding.

To be sure, government funding for R&D rose by about 440% in inflation-adjusted dollars between 1953 and 2006. Currently, two-thirds of that is military funding, though this reflects a post-9/11 uptick; the peacetime norm for federally funded R&D is a 50-50 split between military and nonmilitary R&D. Yet as fast as government-funded R&D funding grew, nongovernment funding grew more than three times faster, from $16 billion to $220 billion, an increase of almost 1,400%. Microsoft alone spends about $6.5 billion each year on R&D, or about twice DARPA's entire annual budget.

At the same time, more R&D is taking place outside the United States. In the early 1950s, the United States and Canada probably accounted for at least half of the world's R&D funding (exact figures were unavailable then for much of the world). Today, 40% of all R&D is undertaken in Asia, compared with 37% in the Americas and 23% in Europe. R&D funding, of course, measures only input, but if one measures output, the results are essentially the same. For example, Asia leads in numbers of "triadic" patents (patents filed simultaneously in the United States, Europe, and Japan) with 36% of the world total. North America accounts for 34% and Europe for slightly less than 30%.

In addition, the United States also is outsourcing an increasing amount of its R&D. Today, that figure stands at 10%. Britain and Germany currently receive the largest shares of this funding, though work outsourced to China and India has been growing rapidly during the past decade.

These trends were inevitable. The growth in nongovernment R&D reflects U.S. economic growth and the burgeoning private sector. Also, as the rest of the world modernized, it was natural for the United States to lose "market share" in R&D, especially given that the population of Asia is 10 times larger.

Even so, such trends have crucial implications for U.S. intelligence. The intelligence community's success in engaging the nondefense, nongovernment, non-U.S. R&D communities has been spotty, at best. The technology that the typical analyst uses today is not much different from what he or she had available 5 or 10 years ago. There are some exceptions: Analysts have access to Intelink (a classified version

KEEP R&D CLOSE ENOUGH TO USERS THAT RESEARCHERS ARE INFORMED BY REAL-WORLD PROBLEMS BUT DISTANT ENOUGH TO THINK OF TRANSFORMATIONAL IDEAS.

of the World Wide Web), chat rooms, instant messaging, and, most recently, Intellipedia (a classified wiki). But these technologies are no better than those available in the private sector, and, significantly, intelligence organizations adopted them after the private sector did.

The intelligence community needs better ways to tap outside technical knowledge and expertise. If it cannot draw on the private sector and foreign R&D, it is shutting itself off from three-quarters of the world's technology base. Opening these new channels presents challenges, mainly in the area of security. But such challenges are hardly insurmountable. The intelligence community has decades of experience working with industry partners, foreign friends, and even some not-so-friendly allies of necessity.

At the same time, U.S. intelligence needs a strong R&D base of its own. Companies in high-technology sectors typically spend 15 to 20% of their revenues on R&D to ensure an independent source of technology and ideas. The Department of Defense (DOD) follows a similar practice. In its $440 billion budget proposed for 2008, the DOD planned to spend $82 billion on R&D, with about $11 billion of this devoted to basic science and technology. Because the intelligence community is smaller and because its dependence on technology is, if anything, greater, it may need to set aside somewhat more than this proportion if it hopes to secure the technological edge it requires.

New R&D model needed

The popular image of advanced R&D is of a world where geniuses see further into the future than the average person and make the future happen today. Indeed, that is how DARPA describes its operating model: acting as a bridge between defense laboratories, which typically plan 3 to 5 years into the future, and technologies that would otherwise be 10 years distant.

This model may have worked well for defense, but there are problems in applying it to intelligence. The probability that the intelligence community will have a unique scientific insight is low. Sheer numbers work against it. Commercial and foreign scientists outnumber those in the intelligence community by several orders of magnitude. Even the DOD, which today funds less than 5% of the world's R&D, is 10 times larger than U.S. intelligence community.

This is not to say that intelligence organizations have not produced some impressive technology. But history says that when they have, they often, perhaps usually, employ a different model using the following tactics:

Borrow technology developed by someone else. The basic technology for the U-2, CORONA, and sophisticated relational databases had all been around for some time when an intelligence organization grabbed the technology and delivered a system faster than others would or could.

Use funding authorities or contracting vehicles innovatively to leapfrog the normal bureaucratic and legislative process. The U-2 was rushed into service using the CIA's special budget authorities. More recently, the RQ-4 Global Hawk unmanned aerial vehicle was built as a prototype under the DOD's Advanced Concept Technology Demonstration program, with the early units essentially constituting operational systems.

Get technology into operation faster by accepting more financial, technical, political, or operator risk. The U-2 achieved its remarkable operating ceiling by accepting flight characteristics and safety margins that would be unacceptable in a standard military aircraft.

Continue a program even after several failures or substantial cost overruns when a system seems promising and important. The CIA's CORONA program had 13 failed missions over 12 months before a success. Its A-12 aircraft (the predecessor to the Air Force's SR-71) exceeded its budget by a factor of two; rather than 12 aircraft at a cost of $100 million, the program delivered 10 aircraft at a cost of $161 million (about $1.2 billion in today's dollars).

Not all programs that use these tactics succeed or prove productive. But when intelligence does succeed, this seems to be the formula at work. Intelligence technological breakthroughs owe more to risk-taking than to sheer genius. This suggests that if the U.S. intelligence is to have a tech-

CREATE GREATER OPPORTUNITIES FOR THE INTELLIGENCE COMMUNITY TO ENGAGE THE BROADER R&D COMMUNITY.

nology advantage, it may be more important to concentrate on managing aggressive risk-taking effectively than it is to search for ideas that no one else has.

On reflection, this is understandable. All R&D is competitive to some degree, but few technological fields are as defined by the pressure of competition as is intelligence. Intelligence R&D success depends not just on making a technology work but on staying ahead of a constantly evolving competitor who is usually trying to make the technology fail. Military R&D has some of this competitive flavor in the shifting balance between offense and defense, but military technologies are mainly reserved for wartime, and so one does not see who is ahead so clearly or as often as in intelligence.

Intelligence culture also rewards risk-taking because success or failure is usually determined at the margin—whether an aircraft can fly 5,000 meters higher than the interceptors pursuing it, or whether a computer used to break a cipher is more capable than the algorithm used to create it. Such a culture tilted toward favoring risk would be inappropriate in R&D for medical devices or commercial transportation systems, but it is essential to intelligence.

Strategy principles

All of this suggests some principles for an effective intelligence R&D strategy.

First, create greater opportunities for the intelligence community to engage the broader R&D community. This effort should include opportunities for intelligence community technical personnel to work for periods in academic or commercial research organizations and opportunities for researchers outside intelligence to work inside. Intelligence personnel especially need opportunities to work abroad, as that is where three-quarters of the world's R&D now takes place.

The intelligence community is at a disadvantage in competing for many of the best scientific minds. A career decision to work in intelligence often isolates a scientist from the broader R&D world, and there are not many opportunities that enable researchers to move back and forth.

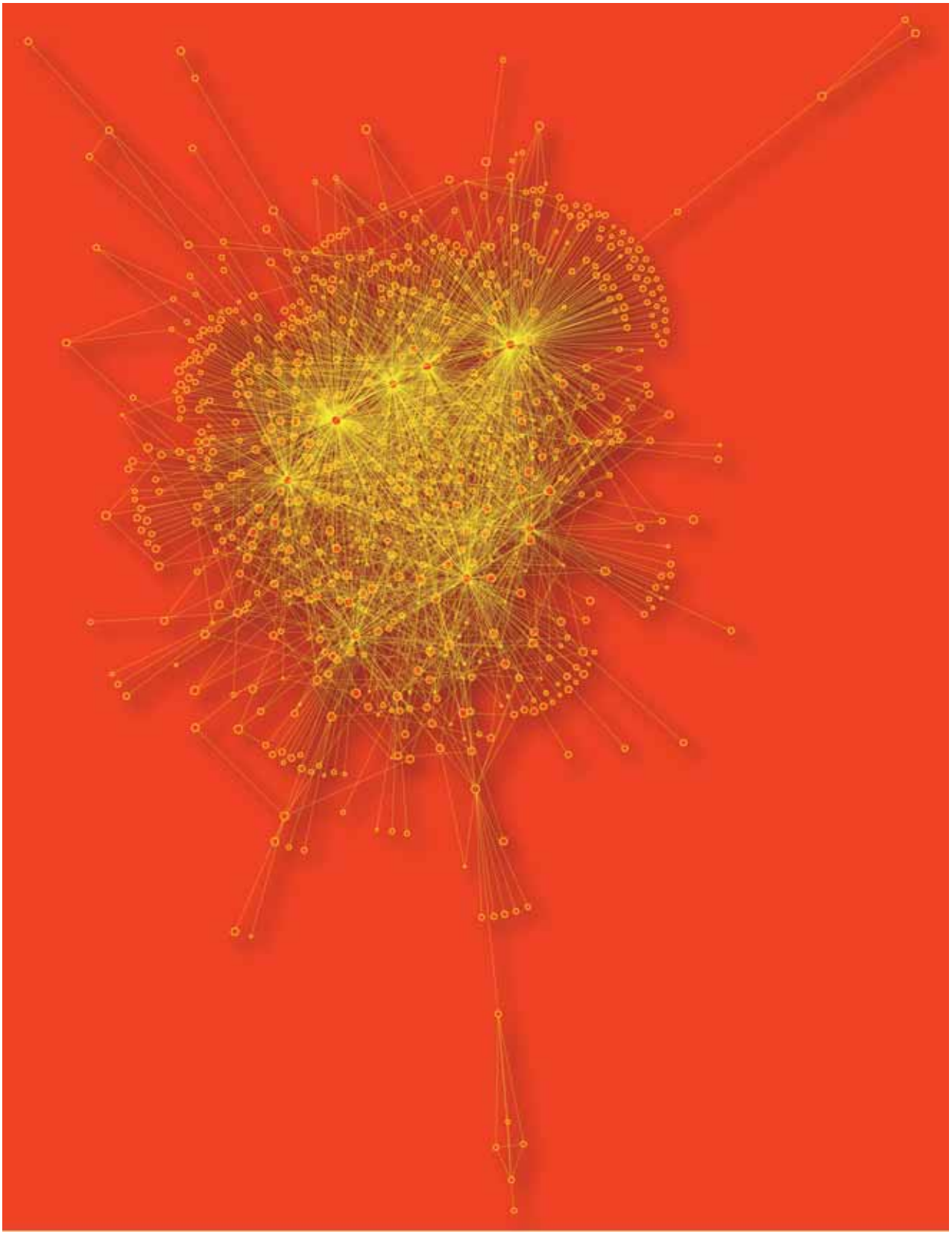
The intelligence community could expand its current graduate and postdoctoral fellowship programs. Most participants would go on to academic or industry jobs. However, they could be given an option to maintain a part-time relationship with the intelligence community (and thus maintain their clearances), much as reserve officers do in the military services. This effort would gradually build a larger pool of cleared scientific personnel who are engaged with the community and might think of opportunities or applications for intelligence. It would keep intelligence on the scope of more researchers.

Second, develop specialized expertise within individual agencies but provide incentives and opportunities for them to work together. Some of the most challenging problems have gone unsolved precisely because they do not fit neatly into any agency's mission. These problems inherently require a multi-intelligence approach, but there are insufficient venues for agencies to collaborate. Examples of such problems include:

Tagging, tracking, and locating. Cold War targets, as noted, were most often missiles, ships, factories, or armies—large targets and often immobile. Today's targets are often individual people, including terrorists and insurgents. Finding them almost always requires a combination of intelligence disciplines. Technology is part of the solution, but a substantial amount of R&D is needed, and the most challenging task may be integrating a wide variety of data sources, tailored to a particular situation.

Detecting and assessing WMD. Advanced technical collection, especially measurement and signatures intelligence, might help in detecting clandestine WMD programs. However, as with tagging, tracking, and locating, the requirements for detecting WMD are likely to vary from target to target and will probably require a combined approach in any case.

Persistent surveillance. Early reconnaissance systems provided only snapshot observation of targets. Networking multiple sensors and a variety of long-lived platforms could make it possible to observe and record data over an area for extended periods. This enables one to detect movement more readily. One can also monitor areas for change and go



CESAR HIDALGO, *Hairball Shadow*, Nodes are disease diagnoses, and links connect diagnoses likely to affect the same patients, 2007.

backward in time to trace the cause of an event.

Analytic tools. Analytic organizations often are too small to develop these technologies on their own and usually lack the expertise to turn an analyst's idea for a labor-saving device into a working technology. Technology developers, on the other hand, often have not fully understood how analysts do their work. Their inventions often have aimed at replacing, rather than facilitating, the analytic process, and analysts are naturally suspicious of any tool whose logic process is a black box.

Networking across agencies and jurisdictions. In 2004, Congress passed an intelligence reform act that called for the creation of an "information sharing environment" that would enable the intelligence community, military forces, law enforcement agencies, and local jurisdiction to exchange data easily. Such a network must work across all intelligence organizations and disciplines. The technology for managing access has not yet been fully proven, and it is not clear who has responsibility for developing it.

Third, keep R&D close enough to users that researchers are informed by real-world problems but distant enough to think of transformational ideas. R&D that is disconnected from the problems that the intelligence community actually is working on is apt to be impractical. On the other hand, R&D driven by approved formal organizational requirements is unlikely to transform organizations.

DARPA balances these two goals by having its researchers drive the agency's agenda but also requiring them to find an Army, Navy, Marine, or Air Force sponsor who will integrate the resulting weapon (if successful) into their force structure and budgets. DARPA allows the researchers to shop their ideas to more than one service and also has found niche customers who needed R&D support because they lacked their own. The most notable niche customer in recent years has been the U.S. Army Special Operations Command, which has as its mission supporting "regional combatant commanders, American ambassadors, and other agencies as directed."

The Advanced Concept Technology Demonstration program has used a similar approach, which was part of the reason why it was possible to deploy the Global Hawk so quickly. Intelligence organizations can use this method, too, and this is another reason to maintain a steady flow of personnel between the intelligence community and the outside world and among agencies within the community itself. Researchers and users at middle levels often are the best ones at finding new ideas and the opportunities to use them.

Fourth, develop incentives and opportunities to undertake aggressive risks and manage them effectively. Currently, R&D is so closely linked to system acquisition that there is little room (or tolerance) for failure. There often is a natural disincentive to take risks when developing a replacement for a system that already is serving a large user base. When programs do take such risks and fail, risky R&D as a whole gets a bad name.

Dedicated intelligence R&D programs can create a space where a career does not end because a high-risk project with a potentially high payoff does not succeed. This kind of safe zone is important because some projects inevitably will fail. Such programs are themselves a risk-management technique because they enable developers to pursue new ideas aggressively without endangering existing capabilities. This is important, because if the intelligence community hopes to attract people with a taste for risk, it needs an organization that provides opportunities for taking risks.

Recommended reading

Bruce D. Berkowitz and Allan E. Goodman, *Best Truth: Intelligence in the Information Age* (New Haven, CT: Yale University Press, 2000).

Bruce Berkowitz, "The DI and IT: Failing To Keep Up With The Information Revolution?" *Studies in Intelligence* (Summer 2003); 67–74.

The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, Report to the President of the United States (Washington, DC: U.S. Government Printing Office, March 31, 2205), available at wmdcommission.org.

Defense Advanced Research Projects Agency, *Bridging the Gap, DARPA Strategic Plan* (February 2005), available at www.darpa.mil/body/pdf/BridgingTheGap_Feb_05.pdf.

Defense Science Board, *Transition to and from Hostilities* (Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, December 2004); see especially Chapter 6, "Identification, Location, and Tracking in Asymmetric Warfare."

Jennifer E. Sims and Burton Gerber, eds., *Transforming U.S. Intelligence* (Washington, DC: Georgetown University Press, 2005).

Bruce Berkowitz (bdb@erols.com) is a research fellow at the Hoover Institution at Stanford University and author of several books and articles on intelligence. He began his career at the CIA and has since served in or worked with most other U.S. intelligence organizations.