NATIONAL DEFENSE
RESEARCH INSTITUTE

This PDF document was made available from www.rand.org as a public service of the RAND Corporation.

Jump down to document ▼

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world.

Support RAND

Purchase this document

Browse Books & Publications

Make a charitable contribution

For More Information

Visit RAND at www.rand.org

Explore RAND National Defense Research Institute

View document details

This product is part of the RAND Corporation monograph series. RAND monographs present major research findings that address the challenges facing the public and private sectors. All RAND monographs undergo rigorous peer review to ensure high standards for research quality and objectivity.

Byting Back

REGAINING INFORMATION SUPERIORITY AGAINST 21ST-CENTURY INSURGENTS

Martin C. Libicki, David C. Gompert,
David R. Frelinger, Raymond Smith

Prepared for the Office of the Secretary of Defense

NATIONAL DEFENSE RESEARCH INSTITUTE

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

RAND® is a registered trademark.

Summary

Armed conflict has always made serious demands on information, whether it is about the disposition of our own forces or the intentions and status of the adversary's. With the advent of modern information systems, the management of information about friend and foe has become a key determinant of how armed conflict plays out. The Department of Defense's (DoD's) information architecture for conventional warfare reflects that fact.

Counterinsurgency, though, differs from conventional warfare. First, whereas the battles in conventional war are waged between dedicated armed forces, the battles of counterinsurgency are waged for and among the people, the central prize in counterinsurgency. Collecting information about the population is much more important than it is in conventional warfare. Second, the community that conducts counterinsurgency crosses national and institutional boundaries. U.S. and indigenous forces must work together. So, too, must military forces, security forces (notably police), and providers of other government services. Sharing information across these lines, thus, has a greater importance than in conventional warfare.

An integrated counterinsurgency operating network (ICON) should, therefore, be different than that which DoD has built for conventional warfare. In this monograph, we outline the principles and salient features of ICON.

Information Requirements

If winning war requires understanding the terrain, winning counter-insurgency requires understanding the *human* terrain: the population, from its top-level political structure to the individual citizen. A thorough and current understanding of individuals and their community can help rally support of the government by allowing the government to meet the needs of the local population. Because insurgents do not identify themselves as such on sight, knowledge at the individual level is often what it takes to make such necessary distinctions.

Even the information required for military operations point to the importance of knowing the community. Relying on relevant operating experience, we generated a list of 160 indicative information requirements. To begin, these can be classified by how they are best satisfied: (1) by intelligence operatives, (2) by operators on patrol, or (3) from the population directly. The results are revealing: only 13 require intelligence operatives; 90 can most naturally be supplied by operators; and 57 come from the population. We also assessed the relative importance of ensuring that the information to satisfy these requirements be of high reliability, delivered in a timely manner, and appropriately secured. In this assessment, reliability was the most critical of the three. Usually, the information to satisfy these requirements had to be either highly reliable or at least vetted by experts. By contrast, security tended to be the least stringent desideratum. Only 2 requirements were of the sort that could not be shared with indigenous forces, while 28 could be shared with anyone.

We concluded that gathering information to counter insurgency requires its own framework and model, which acknowledge the role of traditional intelligence collection but then goes beyond it. As Figure S.1 illustrates, the information required for successful operations rests on three pillars, and each of these pillars, in turn relies on specific sources.

Figure S.1
New Sources of Information
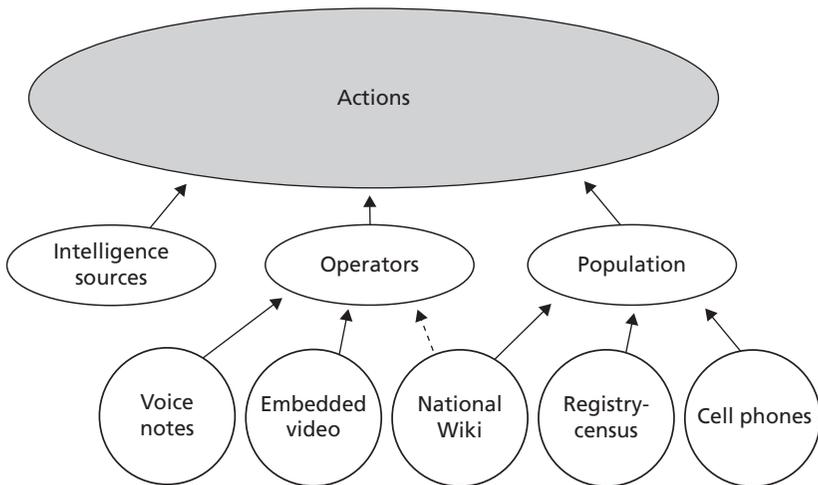
NOTE: Arrows with solid lines suggest primary conduits, while the arrow with the
broken line suggests a secondary conduit.
RAND *MG595/1-S.1*

Collecting Information

The Registry-Census

The most elemental way to learn about the citizenry is to carry out
a registry-census: registry in the sense that the government is taking
names, and a census in the sense that information about people and
where they live is collected and amalgamated. Five lines of information
form the core of a registry-census.

1. *Basic census* information includes: who lives where, their sex
   and age and other basic demographic information (birthplace,
   length of residence, marital status, and ethnic, perhaps tribal or
   religious, affiliation).
2. *Relationships* information covers family ties, notably relation-
   ships to those in different households: siblings, parents, and the
   extended family.

3. *Health* information should cover (1) the mobility status of individuals (e.g., for evacuations), and (2) who has medical conditions that can benefit from state intervention, either routine medical attention (e.g., does this person need to be seen periodically) or in emergencies (e.g., a record of ambulance visits).

4. *Work* information reveals the employment status of a person and, by aggregation, the economic status of, say, a neighborhood or village. It can also serve as a check on (or be served by) a census of establishments.

5. *License* information may include drivers' licenses but also others (e.g., use permits, hunting/fishing licenses, and machinery operation licenses).

Correlated items, incidents data and buildings data, merit attention:

- Incidents data would range from visible crimes to crime reports and nonroutine contacts between citizens and authorities (COMPSTAT—computerized statistics, New York City's master compilation of crime reports, played a large role in reducing the city's falling crime rate in the 1990s).
- Buildings data would be used to construct the national three-dimensional model of the country's built-up areas. Such a model would help define lines of visibility and potential fields of sniper fire, thus, denoting safe or unsafe areas for urban combat, ingress/egress, or convoy operations. It also offers clues as to where insurgents might plant improvised explosive devices and what the terrain looks like in areas that cannot be directly seen. The internals of buildings are relevant when they must be entered either in pursuit or to take cover.

Finally, circumstances may merit the development of a national identification system. While the general purpose of the census-registry is positive in that it represents the data foundation for helping individuals so counted, a national identification system exists to detect those who wish to evade the grasp of authorities, of whom insurgents would

be the critical subset. If identity cards are required at certain times and places, insurgents would have to acquire them, allowing themselves to be tracked, or avoid them, thereby having to avoid checkpoints. In contrast to a census, universality results, not from the application of grunt work but from disincentives to being excluded. This disincentive also applies to those who have crossed the border without encountering authorities; they, too, would excite suspicions when appearing without the proper tokens of identity. To the extent that the existence of a cross-border refuge is correlated with insurgent success, the two goals—smoking out insurgents and illegal foreigners—are correlated.

Cell Phones

If one wants to know how people are moving and interacting on a day-to-day basis, there is no information quite as rich as what the cell phone system routinely collects by the minute. Every time someone makes a phone call, some switch, in the normal course of doing its job, records who is calling, where the caller is, who is being called, where the called party is, and how long the call lasted—that is, the *externals* of the phone call. If the cell phone system, however, is not architected to deliver such information, it will be discarded, thereby leveling the information field, despite the well-founded expectation that authorities backed by U.S. resources should dominate the field. Cell phones, by contrast to most high technology, are ubiquitous in the third world, with more than a billion users and over seven million in war-torn Iraq alone.

Exploiting cell phones would require authorities to:

- Encourage and accelerate cell phone usage,

but

- Shape the cell phone environment in ways that favor authorities.
- Ensure cell phone calls can be associated with registered users.
- Ensure cell phones can be geolocated when used and when otherwise useful,

and

- Acquire and amalgamate cell phone calling and location data to support the delivery of government services, empower progovernment forces, and direct security forces appropriately.

Below we take each requirement in turn.

Encourage Cell Phone Use. Government's job would be to facilitate the build-out of infrastructure and encourage pricing plans that accelerate user growth. Favorable policies may include ready access to spectrum (although spectrum is abundant in developing countries), and some sort of eminent domain for acquiring the land or building rights for cell phone towers and antennae (in developed countries, rights are often more expensive than the equipment). To the extent that cell phone towers are at risk from warfare (especially if the insurgents do not perceive cell phones as their friends), they have to be protected and insured, again, perhaps at subsidized rates. Where violence is constant and no infrastructure can expect to have a very long half-life, the U.S. government could "loan" the cell phone system aerostats or similar equivalents of air-borne transmission towers.

Shape the Cell Phone Environment. Everything important about a cell phone system stems from its software—what goes into the handset and, more importantly, what goes into the switch (e.g., that determine which calls are routed, or which information is retained). To ensure real-time collection, security, and proper distribution, governments should control this software, either by inserting modules into the code base, or developing specifications for the cell phone owner to the same effect. Similarly, government requirements should inform the handset environment—what the user sees when the phone is turned on, and what is invoked with each menu selection. Calls to authorities, including but not limited to 911-like calls, should be topmost. Privileged access, however, can be more broadly extended. Nongovernment groups that do or would support the government (e.g., friendly mosques) can be built into the menu both to be accessed and to deliver services such as sermons-of-the-day. This would not only make it more attractive for such groups to support the government, but those that do would see their power increase over those that do not.

Associate Cell Phones with Registered Users. Phones activated with stored-value cards (typical in the third world) give little clue who is making or getting calls. This limits the intelligence value of externals. Furthermore, if cell phones offer no clue to who is using them, insurgents have no reason to avoid them. One solution to the anonymity problem would require that each phone's subscriber information module (SIM) chip be associated with a particular individual much as a national identification card is. It would be issued in person only when the individual showed up to register for a cell phone. If the switch does not read a SIM as part of the call setup on either end (of a cell-phone-to-cell-phone connection) the call is simply not made and the relevant handset or handsets will be so notified.

Geolocate Cell Phones Periodically and as Needed. Today's phones can locate themselves either triangulating relative to transmission towers or by reading Global Positioning System (GPS) signals. At a minimum therefore, cell phone locations for both sender and receiver would be transmitted when cell phones are looking for service, when calls are placed (whether or not they are connected), and periodically over the course of the phone call.

Even if it does nothing, the surveillance features of the system may well keep insurgents from using cell phones (or at least not without a lot of operational security on their part). But this system *can* do some useful things.

Acquire and Amalgamate Cell Phone Calling and Location Data. This requirement will support the delivery of government services, empower progovernment forces, and direct security forces appropriately.

Government Services. The proliferation of location-aware cell phones facilitates enhanced-911 services. If these cell phones can also be used as cameras, the evidence gathered on the spot can provide assistance that is all the more ready to act upon arrival. A cell phone system could also issue warnings of dangerous activities taking place in neighborhoods.

Eyes on the Street. A proliferation of cell phones, irrespective of all other system measures, means that any given insurgent operation, incident, explosion, or crime witnessed by a large number of people

can be reported on. If the call is made while the activity is ongoing, authorities can be given the location (an improvement in accuracy over users reporting their own location). Camera phones can send pictures of the area to authorities, assisting in sizing up the situation, collecting evidence of what happened and who was responsible, and even identifying possible insurgents.

Actionable Intelligence. A record of phone calls is a start in distinguishing friend from foe. If such phone calls are consistent with appearances in insurgent strongholds, when there is no other reason for presence there, authorities might look further. Conversely, if there is already some intelligence on an individual, the pattern of calls may be further proof—or it may help to establish that someone does *not* merit further scrutiny.

U.S. policy on cell phones recognizes the possibility for the information to be misused. Thus, policies may be needed to restrict to whom the information from the system can be transferred, to make the use of the system transparent, to otherwise restrict how the system is used, and to limit how well the host government can run the system without U.S. help, coupled with technical measures to reduce the utility of the system should the United States find it is being misused.

Finally, a solid reliable cell phone infrastructure can also permit cell phones to be used as the *primary* communications device of U.S. and indigenous operators. Since both will be using the same system, interoperability issues never arise. Indeed, U.S. operators would have a vested interest in and near-instant knowledge of the state of the cell phone system—to the benefit of its protection. Because the features of modern cell phones are converging with those of palmtops, carrying a cell phone can provide easy-to-use forms for data connectivity: e.g., to incidents or wants-and-warrants reports. Because connectivity cannot be guaranteed in a war zone, it would be premature to junk the entire existing army military communications suite. But, because cell phones are light and cheap, why not carry one against the possibility that service may be available? Furthermore, although normal civilian cell phones transmit in the clear, some high-end cell phones already come equipped with the National Institute of Standards and Technol-

ogy's advanced encryption standard–enabled communications, which mask the internals, but not the externals, of calls.

Embedded Video

Following the 1992 Rodney King incident, video cameras began to appear on the dashboards of police cruisers. At first these cameras were resented as symbols of the distrust with which police officers were held. Over time, such cameras became widely accepted. Police officers, continuously aware that they were being recorded, learned to be on acceptable behavior at all times before the camera. The cameras grew to become widely appreciated. No longer could errant citizens falsely claim that they had been abused by the police—as long as such purported abuse had taken place in the camera's line of sight.

The soldiers' equivalent of a dash-board video camera could be a helmet-mounted device or one coupled to the scopes found on most rifles these days. The devices would operate continuously, recording everything and marking critical events, such as a weapons discharge. Soldiers would go on patrol or station with power supplies fully loaded and portable storage empty. When they returned, they would dump portable storage into fixed storage, and recharge or swap out their batteries. The record would be examined between patrols, either by looking at all the material retrieved or by scanning forward to marked events and working from there. The interesting material would be transferred to permanent storage.

The primary purpose of these gun-mounted video cameras is to inhibit behavior with unfortunate consequences among soldiers so that they will take action when warranted or be exonerated and defended when accusations prove erroneous.

An important secondary purpose is as a learning tool in combat, similar to play-action tapes following football games. Abundant material can encourage learning at a low level in the organization, using both direct instruction and the often-more-valuable peer-to-peer instruction that may result from sharing the material throughout the network.

An occasional but valuable tertiary benefit is that the cameras may, from time to time, video people of interest to authorities: e.g., those who may be the ones taking at shot at the troops.

National Wiki

Knowledge of the community is a critical requirement for both long-term stabilization and episodic operations. Indeed almost 20 percent of the 160 data items in Chapter Two require knowledge of the community's social, political, and economic structure.

Normally, militaries gain such knowledge by sending their intelligence operatives to look around and ask questions, which is essential but no more efficient than it was in biblical times—and such operators are "thin" on the ground. Even in Iraq, intelligence officers number in the hundreds, while the total population of operators on the street hardly exceeds 30,000—this in a country with tens of millions of people.

Getting the local population to reveal the ways and means of their respective communities, one person at a time on the street, is hindered by errors in oral transmission, language barriers, lack of operator context, and frequent errors in translation to a records system. In today's information age, there has to be a better way to induce the generation and sharing of all this local knowledge. In fact, there very well may be such a way—Wikipedia may be one such model. One challenge in building what might be termed a national Wiki is to persuade the locals, in large numbers, to volunteer descriptions of their community and in ways that communicate the relevant context and intelligence for others, whether U.S. soldiers or host-country soldiers from out of town. Another challenge is converting a medium made for computers into one that can accept input and generate meaningful material from those equipped only with cell phones. There are potential ways to address each of these aspects.

ICON

What kind of information system should the United States employ to conduct counterinsurgency most effectively? How can the system best serve users (rather than what someone has determined are users' needs)? How best can the qualities of timeliness, reliability, and security be balanced? How can information supplied by the intelligence communities, by the observations of security forces, and by information that only the population can provide be integrated in one system? How can

such information capture the complex dimensions of the human terrain over which insurgencies are fought?

These are people, not technical, issues. First, they involve rules and responsibilities: Who is to gather information, who is to process it, who (if anyone) is to vet it, and who is to determine whether it is good enough to act upon? Because of the crucial but tricky relationship between U.S. and indigenous forces, determining who can see what information is all the more critical. Second, it takes distributed cognition to counter insurgency well. Every insurgency is different, and each is "ill-structured" (i.e., metrics are difficult to define and harder to acquire). Few local solutions can be effortlessly replicated across the entire theater because they differ from one time to the next or from one place to the next.

The following are the principles of ICON:

1. *Emphasize user primacy, inclusiveness, and integration*: counterinsurgency information users should have unimpeded access to whatever data they need to act and unobstructed communications with whomever they need to collaborate. User primacy, in turn, demands that networks be designed and operated for *inclusiveness* and *integration*: inclusiveness because the more participants an information network has the greater its value to each user and integration because internal boundaries frustrate collaboration.

2. *Build ICON to go native*: One and only one network should be the primary host for both U.S. and indigenous forces (plus other coalition forces). Anyone on the network should be able to send messages to anyone else on the network and call on the same (multilingual) tools. If the indigenous forces cannot afford the network, the United States should not stint in this matter.

3. *Audit, audit, audit*: ICON should emphasize auditing what people do with information rather than what information people have. Although auditing requires constant vigilance and cannot promise the kind of assurance that security compartments can, compartmentation has obvious costs. Auditing also has the potential to detect rogue users, not merely deny information

to them. By dint of being active rather than passive, auditing is potentially more adaptive. Some auditing techniques include (1) noting what normal usage is and investigating deviations from that norm, (2) sending somewhat different information to selected individuals so that if it is recovered in the wrong hands, it will be clear why, and (3) inserting into ICON information of the sort that a rogue operator may react to in a different manner than a loyal operator might.

4. *Tune ICON to the level of insurgency*: Insurgents tend to present themselves in one of two ways, depending on their strength. Each way calls for a different manner of gathering information on them. When insurgent strength is limited, insurgents will be clandestine. When insurgent strength grows, insurgents are more likely to be overt. They may be organized in significant units and, while still attempting to hide from detection, have quite a different character about them, in most ways resembling a classic military problem of dealing with small dismounted units in a complex terrain.

5. *Post before process*: Value-added services—such as the caveats associated with the processing of, analysis of, and commentary on information—should be available on ICON—indeed should be as thick as fleas—but they should not be mandatory, irrespective of their value.

6. *Establish a standard deck and populate it from a national Wiki*: e.g., a list of prior operations or interactions, who lead them, how to contact those leaders; which local official is linked to which militias; and which insurgents are active, with what tactics, and exploiting what grievances. The aforementioned 160 requirements can be considered a prototype standard deck, which can be modified for the local circumstances of each insurgency as well as time and place.

7. *Rank information by reliability and relevance*: e.g., a facility by which accurate and relevant information could be noted as such to help users find the information they seek.

Consistent with these principles, Figure S.2 suggests a possible access architecture for ICON.

This emphasis on the thinking user forms the case for ICON's most important principle (user primacy) as well as its fifth principle (post before process), the sixth principle (the standard deck), and the seventh principle (ranking information). The second principle, building ICON for indigenous forces, and the fourth principle, tuning ICON to the level of insurgency, both follow from the argument that, sooner or later, and preferably sooner, an insurgency has to be won by indigenous forces: war fighters but also police, political leadership, and civil servants. Both principles together require a shift away from compartmentation (essentially information denial) as the primary tool of information security and toward robust auditing, the third principle.

Figure S.2
An Access Architecture for ICON
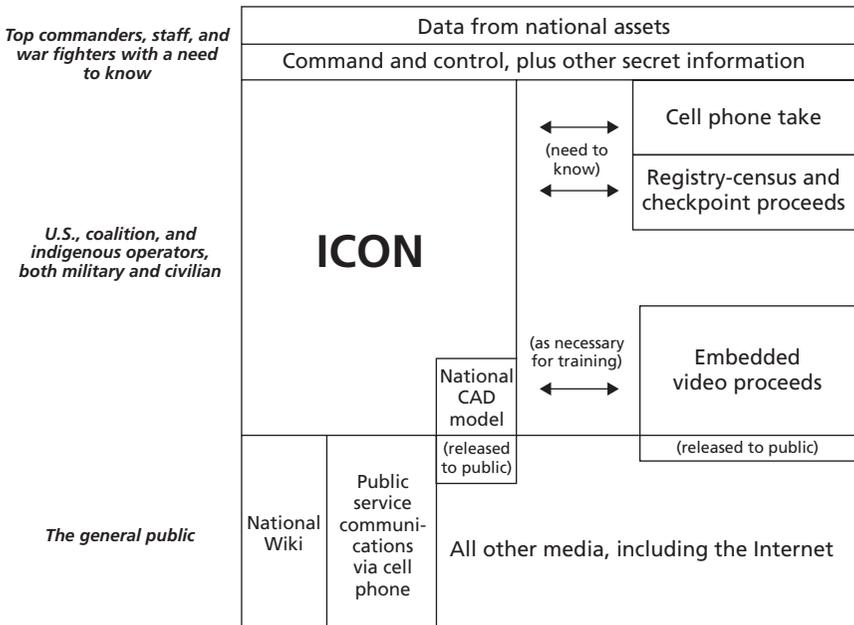
Although the United States would be the principal agent in developing ICON and the information-collection systems described here, the aim is as much to build host-government capabilities as it is to build U.S. capabilities. This aim is in keeping with the idea that successful counterinsurgency depends on convincing the contested population that its government offers a better future than do the insurgents. At the same time, information power can be abused—to the detriment of the very people it should serve—through manipulation, invasion of privacy, and expansion of government power without accountability. Given that the best long-term antidote to insurgency is legitimate, open, and trustworthy government, the last thing the United States wants is to equip local regimes to become information-age police states. In addition to technical safeguards against abuse, the United States should insist on, and contribute to, the development of strong and independent justice systems to check executive power.

Implications and Implementation

Four core ideas have emerged from the larger RAND counterinsurgency project of which this study is a part: First, the main goal of counterinsurgency remains to establish government legitimacy in the eyes of the people whose allegiance is contested by the insurgency. Second, such legitimacy can be undermined by the large-scale presence and use of foreign (notably U.S.) military force in counterinsurgency, especially in the Muslim world. Third, the dangerous fusion of local-political insurgency, criminal activity, and global jihad—as seen in varying degrees in Iraq, Afghanistan, the Levant, and elsewhere—makes it both harder to establish government legitimacy and more essential to reduce reliance on foreign military power. Fourth, the United States should invest in capabilities that can counter insurgency with reduced reliance on U.S. military power, while also enabling lethal force to be used judiciously and precisely when necessary.

Because there is no free lunch, user primacy, inclusiveness, and integration inevitably come at the expense of current security practices. To be sure, no policies should be allowed to make U.S. information sys-

tems, as such, less trustworthy. But opening up information to indigenous partners is necessary, even if it raises the likelihood that some of the information may be abused. The solution is not to keep indigenous partners out of the loop but to establish auditing techniques that rapidly detect the potential for leaks and other abuse. Otherwise, the price paid for not sharing information with these partners will remain steep: disjointed operations, impaired trust, lack of understanding, and delay, not to mention almost certain loss of reciprocal information. The broader policy alternative to security primacy is to achieve advantage through better, smarter, faster, fuller cognitive absorption and use of the information. Note that a large share of the information required for counterinsurgency is about the population—and none of that is particularly secret.

Many of the specific information-collection capabilities we propose to support security operations can also be used as important components of governance, accountability, and public expression. The cell phone system can be used to enhance security on a neighborhood-by-neighborhood basis. Tracking safety officers responding to emergency calls can show how responsive they are. Cell phones can be easily engineered to permit citizens to talk with or write to their government about services. These capabilities are truly dual-use investments; they serve information purposes and government legitimacy.

Finally, we urge that ICON be conceived and nurtured to grow organically, rather than being built as a system per se. DoD traditionally turns to defense contractors (*lead systems integrators*) to buy and assemble information solutions, in part because red tape discourages commercial information technology (IT) firms from entering the defense market. Even the simple idea of getting various U.S. forces to use compatible radios—a 20th-century device—has taken a decade and billions of dollars. Information users have little say in the design and acquisition of current DoD information networks. Conversely, making an ad hoc migration toward an Internet-like system may be the better model; not least because it spurs the early rejection of bad ideas. There will be a demand for the capabilities of ICON that is backed by U.S. dollars. This demand will attract providers, infrastructure, and technology.

No breakthroughs in information science or massive investments in network infrastructure are required to improve information capabilities for counterinsurgency. Nevertheless, the following suggestions could make information capabilities work better:

- Face recognition technology based on likelihood-of-appearance indicators.
- The integration of the various desiderata of the cell phone system into a coherent software suite.
- The integration of near-commercial-quality video cameras into helmets, rifles, and other portable gear.
- Methods of porting the Wiki model to cell phones.
- Improved indexing and categorization of incidents, observations, and other material relevant to counterinsurgency.
- Automated relevance and reliability-ranking methods.
- Improved techniques for auditing computer usage for signs of suspicious activity.
- Human behavior and learning research to improve our understanding of how users might be trained to make effective use of ICON, notably in countering insurgency.

Conclusion

Notwithstanding the fact that only modest extensions of information technology and infrastructure are needed to create ICON and associated data-collection systems, the difficulty of doing so should not be underestimated. In addition to designing and engineering work, DoD and leading IT firms will have to work together as they never have before to crack such problems as providing selective security in an open search-collaborative environment. With proper incentives, market forces will provide most of the drive needed. But an abundance of creativity and common purpose will also be needed.

The United States is the unrivaled leader in virtually every aspect of information networking. It leads in the core sciences, the hardware and software, the products and services, and the market dynamics that

drive it all. It has led the way in creating a global information infra-structure. Its technology and service providers have shown remarkable creativity and sensitivity to users' needs. While the U.S. national secu-rity establishment has been a straggler for the last two decades or so, it is beginning to find its stride in applying IT and network principles to warfare, and it is attempting to remove bureaucratic, cultural, and regulatory obstacles. Gaining advantage on the information level of counterinsurgency is possible, but it will take focus, commitment, and cultural-institutional transformation.