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.

RAND COUNTERINSURGENCY STUDY • VOLUME 1

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

RAND NATIONAL DEFENSE RESEARCH INSTITUTE

The research described in this report was prepared for the Office of the Secretary of Defense (OSD). The research was conducted in the RAND National Defense Research Institute, a federally funded research and development center sponsored by the OSD, the Joint Staff, the Unified Combatant Commands, the Department of the Navy, the Marine Corps, the defense agencies, and the defense Intelligence Community under Contract W74V8H-06-C-0002.

Library of Congress Cataloging-in-Publication Data is available for this publication.

ISBN 978-0-8330-4189-0

Cover Image by Amir Shah, Courtesy of AP Photo

Cover Design by Stephen Bloodsworth

Published 2007 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665
RAND URL: http://www.rand.org
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

Preface

A primary output of the RAND Corporation's research project for the U.S. Defense Department on how to improve U.S. counterinsurgency capabilities, this monograph should be of interest to the U.S. government and other countries and organizations now rethinking counterinsurgency strategies and retooling counterinsurgency capabilities in view of developments since September 11, 2001. It should also be of interest to scholars trying to understand continuity and change in this field.

The larger RAND project of which this is part will yield a stream of products during its course, culminating in a final monograph that draws on that stream of work. Thus, this particular monograph can and should be read both as an output, in and of itself, and as a piece of a larger picture of RAND's counterinsurgency work.

The topic of this monograph, information capabilities for counterinsurgency, has not been heavily analyzed even though there is a great deal of attention paid to information capabilities for conventional warfare. We argue that the information collection requirements and systems for counterinsurgency matter as much as they do for conventional warfare but that they have to be quite different, for two reasons. First, because the community that conducts counterinsurgency crosses national and institutional boundaries, sharing information across these lines has a greater importance than in conventional warfare; security rules that impede such sharing may have to yield. Second, because the indigenous population plays a much greater role in determining the outcome of an insurgency, collecting information about this popula-

tion has a far higher priority than it does in conventional warfare in which the enemy is the focus. We then demonstrate what this alternate focus may imply for requirements, collection, networking, and systems design.

This research was sponsored by the U.S. Department of Defense and conducted within the International Security and Defense Policy Center of the RAND National Defense Research Institute, a federally funded research and development center sponsored by the Office of the Secretary of Defense, the Joint Staff, the Unified Combatant Commands, the Department of the Navy, the Marine Corps, the defense agencies, and the defense Intelligence Community.

For more information on RAND's International Security and Defense Policy Center, contact the Director, James Dobbins. He can be reached by email at James_Dobbins@rand.org; by phone at 703-413-1100, extension 5134; or by mail at RAND, 1200 South Hayes Street, Arlington, Virginia 22202-5050. More information about RAND is available at www.rand.org.

Contents

Figures

Tables

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.

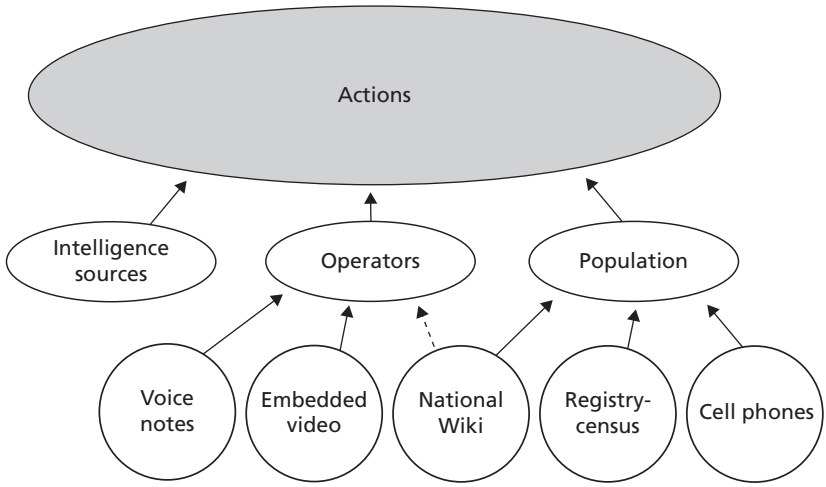
Information Requirements

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 relationships 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

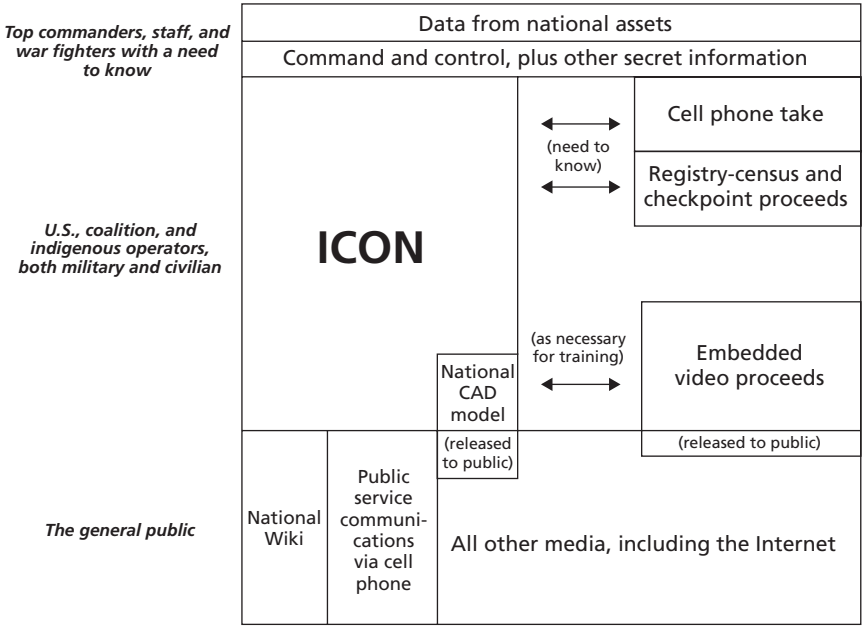
to them. By dint of being active rather than passive, auditing is potentially more adaptive. Some auditing techniques include (1) noting what normal usage is and investigating deviations from that norm, (2) sending somewhat different information to selected individuals so that if it is recovered in the 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



RAND *MG595/1-S.2*

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 infrastructure. Its technology and service providers have shown remarkable creativity and sensitivity to users' needs. While the U.S. national security 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.

Acknowledgments

To begin, we extend our appreciation to our sponsors, Mike Higgins and Ben Riley from the Office of the Secretary of Defense. Both provided valuable guidance for our research and offered very helpful comments in their reviews of our products.

We also thank our RAND colleagues: John Gordon and Jim Dobbins read our manuscript carefully—both of them gave us useful advice on its content. Bruce Don and David Signori were our reviewers—their careful attention to our arguments and suggestions for further improvement were cogent, intelligent, and to the point. Our manuscript is much better for their intervention. Assistant Chief of Police Jim McDonnell and Deputy Police Chief for Counterterrorism Mike Downing, both from the Los Angeles Police Department, offered us insights into the relationship between policing and the topics we raise in this monograph.

At RAND, we also thank Lesley Anne Warner for her assistance in helping complete the monograph, Christina Pitcher for detailed editing, and Susan Bohandy for her writing and organizational efforts, which were invaluable in communicating our findings in the final book.

Abbreviations

AES	advanced encryption standard
AO	area of operations
CAD	computer-aided design
COIN	counterinsurgency
COMPSTAT	computerized statistics
DoD	Department of Defense
EB	*Encyclopaedia Britannica Online*
GPS	Global Positioning System
ICON	integrated counterinsurgency operating network
IED	improvised explosive device
IT	information technology
KIA	killed in action
MIA	missing in action
NGO	nongovernmental organization
OGA	other government agency
PIN	personal identification number
RFID	radio-frequency identification device

SIM	subscriber information module
TPED	task, process, exploit, and disseminate
TPPU	task, post, process, and use

CHAPTER ONE

Introduction

Armed conflict has always made serious demands on information, whether regarding the disposition of our own forces and resources or intentions and status of the adversary's forces. With the advent of modern information systems, the management of information on friend and foe has become one of the more important determinants of how armed conflict plays out. War-fighting networks have assumed corresponding importance within a military's overall war-fighting architecture. The Department of Defense's (DoD's) information architecture for conventional warfare reflects that fact.

Counterinsurgency, though, differs from conventional warfare in many important respects. Whereas conventional war is waged between dedicated armed forces, the battles of counterinsurgency are waged for and among the people.[1] Whereas the people are a backdrop to conventional conflicts, they are the central prize in counterinsurgency. It is because of these differences that the information systems required to support counterinsurgency are likely to differ as well.

We note two corresponding differences in the requirements for information systems. First, the community that conducts counterinsurgency crosses national and institutional boundaries. U.S. and indigenous forces must work together. So, too, must military forces, other security forces (notably police), intelligence services, and civilian pro-

[1] See Rupert Smith, *The Utility of Force* (New York: Knopf), 2007, for a provocative discussion of some of the implications of war among the people. While he discusses far broader issues than counterinsurgency, many of his insights are quite useful within this domain as well.

viders of other government services. These requirements suggest that sharing information across these lines has a greater importance than in conventional warfare. The design of and policies governing information systems cannot help but be greatly affected by the need to share information outside the U.S. national security community.

Second, because the indigenous population plays a much greater role in determining the outcome of an insurgency than it does in conventional conflicts, collecting information about this population is much more important than it is in conventional warfare, in which the enemy, instead, is the focus. This different focus has many implications for the collection, management, and use of information about a country's citizens. Indeed, the public's attitude toward and acceptance of such practices can have a profound effect on the perceived legitimacy and effectiveness of the government.

What follows in this volume, part of a broader RAND study on insurgency, reflects these two themes. Articulated here are the critical components of an integrated counterinsurgency operating network (ICON). We regard this monograph as a vehicle for ideas that are novel or could use further emphasis in today's counterinsurgency environment. We investigate why and how a system that uses such ideas might be useful, as well as fundamental architectural attributes of a system that may incorporate them. However, this monograph does not contain a comprehensive blueprint for a complete information system; it is not a collection of specifications based on a set of requirements, all or most of which have to be met.

Why Information Superiority Matters in Counterinsurgency

In a conventional conflict, the U.S. military uses information for many purposes, notably to select, locate, and fire on enemy targets accurately enough for particular military effects. The goal of U.S. forces is almost always one of managing collateral damage while maximizing effects for a given level of force. Since our foes operate under other constraints, lack many types of advanced weapons, or carry out some operations

less for military and more for psychological effects, they require a different sort of information. They often focus on knowing U.S. strategies, weaknesses, location of targets, and behaviors, as well as capitalizing on their in-depth knowledge of the local conditions, population, and society to obtain their desired effects.

In counterinsurgency, the primary field of battle is the minds of the active citizenry. The contest between insurgents and the authorities is largely a matter of persuading the population to support their side: Who is right or wrong? Who will give me a better life? Who can protect me better? Both sides appeal to individuals for operational intelligence. The essence of counterinsurgency, therefore, is not armed conflict between U. S. and insurgent forces but a multifaceted security and economic effort that puts the government in a position to serve its people, protect them from insurgent violence, and, thereby, earn their loyalty. Military power has more complex and subtle purposes in counterinsurgency than in conventional warfare: to protect the contested population, its economy, and its infrastructure; to destroy insurgent forces and will; to weaken popular support for insurgents; to inhibit factional or sectarian hostilities; to bolster faith in local government by enforcing law, order, and justice. According to our own soldiers, engaging the local population, improving public safety, and knowing "the street" depend vitally on timely and reliable information.[2]

This concept is worth remembering in face of the argument that the current emphasis on winning at irregular warfare mandates a *de*emphasis of information technology. To be sure, information technology greatly improved the operational performance of high-intensity, high-speed expeditionary warfare units operating against the military forces of hostile states such as the Taliban and the Baathists. When forces are networked,[3] enhanced maneuverability, agility, survivability, and

---

[2] Major Paul T. Stanton, "Unit Immersion in Mosul: Establishing Stability in Transition," Military Review (July–August 2006), pp. 60–70. As of June 11, 2007: http://usacac.army.mil/CAC/milreview/English/JulAug06/Stanton.pdf.

[3] Networked forces, however, are not always the case. During Operation Iraqi Freedom, many soldiers with very little connectivity to the Global Information Grid were still detecting enemy the old-fashioned way—by running into them. See David Talbot, "How Tech Failed in Iraq," *Technology Review* (November 2004), pp. 36–45.

discriminating lethality tend to follow. These capabilities allow U.S. forces to focus on rapid and decisive operations in a way that tends to drive many aspects of our military operations and our thinking about how force is to be used.

Such attributes are not central to countering insurgencies (or, more generally, any struggle where decisive military actions are not central to outcomes). However, it hardly follows that "boots on the ground" not "bits on the network" are what count or that the importance of an adequately sized ground-force contingent overwhelms its need to be well-informed.[4] Such thinking ignores the nature of current insurgent threats—dispersed, hidden, mobile, shrewd, urban, changing. It also gives short shrift to the benefits of information in mastering complexity, outsmarting the adversary, and learning in action. Whether the field of action is on the street or in the minds of the citizenry, the ability to disperse forces, delegate authority, improvise operations, work across organizational boundaries, and make difficult yet urgent decisions matters when operating against scattered irregular forces and matters as much or more so than when fighting concentrated regular ones. To the extent that deficits in information cannot be made up by surpluses in firepower—lest the population be antagonized and the enemy's ranks swell—information may be *even more* critical. There is abundant reporting from Iraq to the effect that when U.S. forces lack timely and reliable information, as is all too often the case, they depend that much more on heavy armor and aggressive raids that have a low payoff and that sour relations with the population. This dependence flies against the growing understanding that such actions are the antitheses of effective counterinsurgency, in which the use of force needs to be dictated by what it takes to support the host government.[5]

---

[4] It is something of a false choice even to pose this as a sort of either, or question. IT systems are by no means a replacement for an adequately sized force, but we think that they can allow for the use of forces in a way that improves their prospect of success, and allows for a force properly sized for long-term operations in support of host governments to be employed to good effect.

[5] The latest U.S. Army/U.S. Marine Corps joint manual on counterinsurgency (Headquarters, Department of the Army (and Headquarters, Marine Corps Combat Development Command, Department of the Navy, Headquarters, United States Marine Corps). *Counter-*

The broader RAND study of counterinsurgency reiterates the importance of reducing U.S. reliance on the use of military power to counter insurgency in the Muslim world, where such power is not generally welcome and can inflame Islamic insurgency.[6] This paradox of force is especially acute when countering jihadist insurgencies, the premise of which is that Muslims everywhere are under attack by U.S. and allied forces and must be defended by desperate means, including suicide terrorism. Force can validate the jihadists' premise and increase their appeal; it can expand insurgency by motivating new insurgent recruits, steel insurgents' resolve and fuel their fanaticism, antagonize the population, and undermine the legitimacy of the very local government counterinsurgency is meant to bolster.

By contrast, information power is likely less risky, putatively more cost-effective, and certainly more conducive to "winning hearts and minds" than heavy force. Well-informed operators can work with greater finesse, which is precisely what is needed in conducting military operations amid a population we are trying to win over. Confident interaction with a population one knows may even protect forces better than relying on blind "force protection" from an unplumbed threat.

We caution, though, that while access to abundant useful information is necessary, it is only half of the equation.[7] If two sides have comparable information, the one with more advanced abilities to sense, learn, and decide will have an advantage. Information is a tool, but

---

insurgency (Washington, D.C.: Headquarters, Department of the Army, Field Manual No. 3-24 (and Headquarters, Marine Corps Combat Development Command, Department of the Navy, Headquarters, United States Marine Corps, Marine Corps Warfighting Publication No. 3-33.5, December 2006), p. 3-1) states: "Effective, accurate, and timely intelligence is essential to the conduct of any form of warfare." This maxim applies especially to counterinsurgency operations; the ultimate success or failure of the mission depends on the effectiveness of the intelligence effort.

[6] The other main alternatives to large-scale physical military power are using nonmilitary ("soft power") instruments and improving local security services.

[7] Improving the cognition of counterinsurgency operators is the subject of a parallel study within the RAND counterinsurgency project. See David C. Gompert, *Heads We Win—The Cognitive Side of Counterinsurgency (COIN): RAND Counterinsurgency Study—Paper 1* (Santa Monica, Calif.: RAND Corporation, OP-168-OSD, 2007). As of June 11, 2007: http://www.rand.org/pubs/occasional_papers/OP168/

the user needs to know how to wield it. Unfortunately, jihadist insurgents in Iraq, Afghanistan, Pakistan, the Levant, and elsewhere seem to make better use of the information available to them in support of *their* strategies than do forces countering them, despite the latter's more advanced information systems. Local awareness and face-to-face contacts give insurgents a head start over foreign forces. With easy access to public information infrastructure—especially cellular networks and the Internet—they can operate in distributed but connected cells, reduce their vulnerability, increase their lethality, communicate with the contested population, learn from global insurgency experience, and exploit media coverage, all the while hiding their tracks in the Internet. Insurgents' connectedness also gives them a sense of being at one with an oppressed Muslim community worldwide. It provides pathways to evoke outrage at images of Western atrocities and to spread the words of charismatic jihadist spokesmen. Against such networked and savvy adversaries, information power has to be more important than firepower.

Because networks enable insurgents to distribute themselves, counterinsurgents should also be distributed, and their information systems should adjust accordingly. Experience in Iraq suggests that ponderous U.S. forces operating under strict control according to tight scripts are a poor match for numerous small, slippery insurgent cells that blend into the contested population. Vertical chains of command, stove-piped organizations, and centralized decisionmaking hinder both responding to dispersed insurgents and engaging the population. Immersion, sensitivity, flexibility, and initiative are key features of effective counterinsurgency. A veteran of Iraq argues that "decentralizing command helps to quickly develop an accurate picture of the situation."[8] Small counterinsurgency units are a better match for the insurgents and work more easily with local security services, provided the leaders of such units have both the information and the latitude to make judgments.

A central challenge of counterinsurgency is to coordinate military action, law enforcement, economic development, institutional develop-

[8] Stanton, "Unit Immersion in Mosul: Establishing Stability in Transition," p. 62.

ment, humanitarian care, etc., without relying on central control and incurring its stifling effects on initiative and responsiveness, which are so crucial in counterinsurgency. It is hard to see how the requirement that operations be at once decentralized *and* integrated can be met without information networks. Networks facilitate integration by permitting horizontal collaboration, assuming all players understand the common strategy and are permitted to collaborate. Yet, what networks giveth in the potential to integrate and include, bureaucratic barriers and security compartmentalization too often can taketh away. Accordingly, this study gives as much attention to the *rules* governing sharing as it does to the technologies that make it possible.

Getting to Information Superiority in Counterinsurgency

In sum, many attributes of counterinsurgency distinguish it from conventional warfare in ways that require commensurate changes in information systems:

- The fact that the terrain of counterinsurgency is the population
- The multitude of actors (not least being the population itself): U.S. military forces, U.S. intelligence sources, contractors (many providing security services), coalition partners, nongovernmental organizations (NGOs), indigenous military forces, indigenous security forces,[9] indigenous civil servants, indigenous political leaders (some of whom may be tribal or sectarian), local militias, and insurgents (those willing to cooperate with the government in some areas while contesting it in others)
- The distributed, adaptive, and fluid nature of today's insurgencies
- The critical role of information operations (battles won on the ground can be lost in the airwaves)
- The potential of force not only to weaken but also to strengthen an insurgency.

[9] Which themselves may be many and various. Besides the Iraqi police, there is another force of 150,000 people, the Iraqi Facilities Protection Service.

These various differences between regular warfare and counterinsurgency mean that information capabilities for one cannot be assumed sufficient for the other, as if it were a "lesser-included" case. Things are not as simple as transporting network concepts and tools from regular force-versus-force combat. To meet the requirement for integrated strategies and execution involving a multitude of actors, ICON should be able to reach out to all of them rather than limit itself to U.S. forces. With cognition and agility so critical, no barrier to rapid information access, whether imposed deliberately or through poor design, can rest unchallenged. Because force can be counterproductive, an information system built to optimize its application, or even its precision application, may be missing the point. Indeed, the heart of successful counterinsurgency—enhancing the legitimacy of and loyalty toward the embattled state—makes it critical to exchange information with the population in order to help address its needs and fears. Legitimacy depends less on body counts than on the equivalent of vote counts—popular perceptions, sentiments, and sympathies. This need puts a premium on having, sharing, and making sense of information in the complex and dynamic sociopolitical environments of most insurgencies, and on knowing when, where, how, by whom, and against whom to use force.

Information requirements for both long-term counterinsurgency campaigns and for episodic counterinsurgency security operations indicate the volume, scope, and nature of demand. These requirements should, and in this study do, inform where and how information can be sought: e.g., intelligence services, databases, local authorities, prisoner interrogations, the local population, and information users themselves. Traditionally and institutionally, military operations tend to rely heavily on secret intelligence secretly gathered from secret sources. But military operations are only one part, and at that a subordinate part, of counterinsurgency. It is at least as important to acquire information from the local population and from information users.

Overview

Our monograph proceeds in four parts: an examination of some of the information requirements of the counterinsurgency mission (Chapter Two), new information and sources that can address these needs (Chapters Three through Six), how these might be put together in a practical way (Chapter Seven), and implications and implementation (Chapter Eight). The latter examines whether the sources and network recommended can meet the requirements posed and suggests specific steps toward the goal of improving the information side of counterinsurgency.

Although it is still very important to understand those who are trying to kill U.S. forces, success at counterinsurgency also requires copious data about the civilian human environment at the individual, community, and national level. The need to achieve a proper balance between these two types of requirements has profound implications for the kind of information and information capabilities counterinsurgents need.

Thus, much of this study is concerned with gathering information, of the sort not hitherto considered a core capability of counterinsurgency: building a robust cell-phone system, conducting a registry-census of the population, making video camera electronics an essential component of weaponry and vehicles, and developing a national Wiki (where citizens describe their community).[10] In each case, we describe how these means directly benefit security *operations* (e.g., cell phones provide intelligence and a lower-risk way to collect tips), but with appropriate attention to how such systems can improve governance (e.g., cell phones permit enhanced 911 services).

The authors do not claim that such concepts will in and of themselves be decisive, but it would be unwise not to avail ourselves of advantages when they appear. We need to keep in mind that 21st-century insurgents are increasingly adroit at obtaining, using, and manipulating information, locally and globally. Staying even, let alone gaining

[10] A Wiki is server software that allows users to freely create and edit Web page content using any Web browser. A Wiki supports hyperlinks and has a simple text syntax for creating new pages and cross-links between internal pages.

an advantage, will not be easy for the world leader in technology. Yet, we have little choice but to challenge the information terrain, and use it to the fullest extent possible to counter information-age insurgencies of this century.

CHAPTER TWO

The Influence of User Requirements

As noted, the purpose of this monograph is twofold. One is to explore ideas that are, if not novel, at least deserving of further emphasis in supporting counterinsurgency. Two is to develop some fundamental parameters to guide the development of an ICON.

This chapter discusses information requirements in support of these two purposes. Consistent with the theme of the overall RAND counterinsurgency work, we conclude that a counterinsurgency is first and foremost a war "among the people."[1] As such, it requires information about the people and their society if it is to conclude well. It also calls for ways to organize such information and make it available, in ways that are less consistent with conventional warfare (where information about the belligerent parties is emphasized), and more consistent with counterinsurgency as the provision of security services.

War, both conventional and irregular, has always involved the search for superiority in the information realm so as to improve operations in the physical world. The tools for achieving objectives in the information realm are matched to the unique demands for information in each realm. Conventional warfare, with its demands for information on the adversary and our own forces, are increasingly tied to sensors designed to detect targets of military interests (tanks, aircraft,

[1] Smith, *The Utility of Force,* p. 271, describes one of the six major changes in warfare this way, "We fight among the people, not on the battlefield." "War among" describes a conflict embedded within a population, as distinct from a conflict on a battlefield, which affects a population. In our assessment, Smith's description well characterizes counterinsurgency and succinctly captures a key element of the environment.

ships, and formations of forces). Irregular warfare, while demanding information on the adversary, entails a much greater focus on information on the population. Many of our traditional sensors do not do this efficiently, and so it is both easier and more reliable to gather information from the people themselves. One way is through technologically mediated interactions such as via cell phones, or from other information technology that provides useful insights to both the population in aggregate and the needs of each individual.

The purpose of discussing requirements is to get a general calibration on the sort of information needed in one of the more demanding sorts of operations and to gain some understanding as to where the necessary information might be gathered in some detail so that ICON can then be evaluated against those demands. We chose to examine information requirements associated with security operations since they represent the most challenging situation in terms of the demands for timeliness, accuracy, and security and since they were best aligned with what the military would be able to produce with its traditional war-fighting and intelligence systems.

When the Population Is the Terrain

Winning a war requires understanding the terrain. In a conventional war, the terrain can be interpreted literally as ground; no soldier would willingly go to war without a map. In counterinsurgency, the primary terrain is the population, from its top-level political structure to the individual citizen. To echo Carl von Clausewitz, insurgencies are politics by other means. Many are resolved through changes in political arrangements, some violently imposed, others negotiated. Because politics is central to insurgencies, popular opinion cannot be ignored. In societies in which other political outlets lack credibility, the decision to support the insurgency or support the government is often how politics are expressed.

In great contrast to conventional war fighters, insurgent war fighters do not identify themselves as such on sight. Those of the other side, authorities, thus cannot easily distinguish insurgents from everyone

else. Detailed knowledge of the population, at the individual level, is often what it takes to make such necessary distinctions (as well as similar distinctions between law-abiding citizens and criminals or members of criminal organizations). Such considerations, for instance, inform the emphasis we place on carrying out a thorough census (see Chapter Three). It also helps in identifying those individuals who have and are willing to divulge useful information. This much can be illustrated by examining, in turn, security operations, improving intelligence and situational awareness, and operations designed to enhance the legitimacy of the host government.

Security Operations

We start off by examining something as simple as conducting a raid on a building, which would seem to require little information other than knowledge of the quarry and the topography of the operation. But doing so without stumbling an unforeseen way or alienating residents requires a sense of who occupies the building (especially in relationship to the persons being sought); what activities are licensed in the location; and, to some extent, who might be employed there or absent for being employed elsewhere. Guarding a building or manning checkpoints also hardly requires much information—but knowledge of what incidents have taken place in the neighborhood recently would provide a clue as to what to look for and what to ignore. Protecting a community is aided by information on who lives there and who is related to whom (such information establishes what normal conditions are and who is likely and unlikely to pass by); who works there; and, finally, what has been happening there lately. When it comes to investigating attacks on individuals, it helps to know who they are and how they are related to others. Operations that involve drivers—such as setting up checkpoints, running convoys, and controlling land borders—benefit not only from incident data but also access to various forms of drivers' licenses and vehicle registrations. Carrying out the latter, border control, also means finding out who the locals (and, to some extent, their out-of-town relations) are, so that they can be treated as locals if encountered. Because prison management (at least in the United States) is often a matter of controlling the prisoners' group dynamics,

it helps to understand the relationship between the incarcerated and the insurgents.

There is an important relationship between information needed and the types of operations being conducted. The more violent operations that are closer in nature to conventional warfare tend to require information that is also more conventional in nature, such as intelligence and topography. But when a counterinsurgency evolves away from the managed delivery of violence—as it should—and shifts toward protecting and building relationships with locals, its operations more resemble police work in terms of the types of and ways that information is used and shared among the security forces and the government. This resemblance is doubly so when security forces address threats to security from street and organized criminals as well as insurgents. In a nutshell, intelligence information loses its relative value compared with information necessary for effective governance. Consequently, information sources and distribution methods that maximize collection and dissemination of governance-related information rise in their importance relative to traditional intelligence sources and distribution channels.

Situational Awareness

Although the pursuit of situational awareness is rarely an end in itself, success is a prerequisite for many types of operations. Enhancing these operations, given the problems of counterinsurgency, requires focusing on the individual and the community, and not on building the kind of order of battle assessment more germane to conventional military operations. A baseline of information on the community and individuals is essential if we are to even begin to ask the right questions, so that other operations can be supported.

Consider, for instance, an operation directed at a village where a reconstruction team and security element might be deployed for an extended period of time. The more you know about a neighborhood or village, the better the clues on whom to ask and how to ask them for information and the easier it is to collect information from its residents. Such knowledge can help indicate what bits of information are meaningful and how to follow up. Thus, when making street-level inquiries it

helps to know who the respondents are and how they fit into the overall community (whether the physical community or one that is defined in terms of relationships); their work status also helps define them. Insofar as many of the conversations are likely to be about recent incidents (as it would be in police work), there should be a thorough knowledge of such incidents. Locating individuals is an activity informed by who is who and who is related to whom (it also helps knowing whom *not* to ask). When conducting forensics after an incident, it helps to know who the people in the neighborhood or village are and how to place the crime within the context of similar incidents in the area. Sometimes health information on the victim or knowledge of the victim's relatives illuminates the nature of the crime, or whether it was a crime at all. Knowing who is who and who is related to whom helps when recruiting friends and relatives of existing insurgents. Interrogators who know a person's identity, residence history, relatives, health status, and prior job history have a leg up on those being questioned.

Winning Allegiance

The ultimate objective of the counterinsurgency effort is to enhance the government's legitimacy and support from the population it serves. A detailed understanding of individuals and their community can help rally support for the government by allowing the government to meet the needs of the local population. Knowing each person's name, relationships to others, health, and job makes it easier to frame the government's case because it can suggest what points that best resonate with him or her. One of the most effective ways of winning local allegiance is by providing health care to those without it. Demonstrating recurrent interest in each individual's health entails knowing who is being served and the medical records that indicate how. Health information, notably who is immobile, can also be critical in evacuations (cf., Hurricane Katrina).

To a large extent, the course of an insurgency is the amalgamation of individual choices. Because specific people have individual concerns, are variously responsible for their actions, and hold a variegated take on the insurgency, the more we understand each person as an individual,

the better we can predict who can be trusted and the easier it is to tailor security services to their individual or community concerns.

Military Operations During Counterinsurgency

Although the great bulk of what it takes to counter insurgency is to provide security and other government services, when an insurgency becomes capable of massing forces in numbers that can overcome police, military responses may be called for. When the insurgency has become strong enough to control rural districts, cities, or at least neighborhoods, military operations are indispensable in reestablishing government control.

This section, thus, focuses on the military operations component of counterinsurgency. Apart from ensuring that the parameters of ICON cover all the important aspects of counterinsurgency, the section's purpose is to test the parameters against military necessity. It might be argued that since ICON supports military operations, it should, therefore, support the same parameters that any military information system supports. Thus, when today's military systems support a high level of information security and compartmentation, so too should ICON. Conversely, if there are important differences between the military operational requirements of counterinsurgency and corresponding requirements of conventional warfare, such differences should inform or at least permit differences between ICON and today's military information systems.

To develop a list of information user-requirements, we relied on the relevant operational experiences of participants in the study. A list of 160 requirements (appearing in the Appendix) is meant to be indicative, not comprehensive. For each requirement, we assessed the relative importance of ensuring that the information to satisfy these requirements be (a) of high reliability, (b) delivered in a timely manner, and (c) appropriately secured.[2] Acknowledging that the culture of the area,

[2] For a discussion of metrics for reliability of information, both in terms of objective metrics and fitness for use metrics, see also U.S. Department of Defense, Office of Force Transfor-

the sophistication of the insurgents, and the particulars of the environment would affect the specific evaluation, we nevertheless thought in terms of a generic scenario to rate each of the three as a "1," "2," or "3," with "1" being most critical, and "3" least.[3] We also judged what the best source for information would be to satisfy each requirement.

Because the main purpose of information is to improve decisionmaking, these requirements can be grouped into the kind of decisions that can be made more confidently with information to satisfy such requirements:

- what and whom to bring to an area of operations (requirements 1 to 8)
- who should be trusted there (9 to 82)
- how warfare should be conducted (83 to 123)
- how insurgent capabilities and intentions can be judged (124 to 138)
- how to carry out specific activities (139 to 158)
- when to leave (159 and 160).

For the resulting aggregate assessments of timeliness, reliability, and security, with all due caveats for the subjectivity inherent in such evaluations, see Table 2.1.

In general, the rankings seem to be correlated across categories: those categories that had the most stringent requirements for timeliness had the most stringent requirements for reliability and security, as well. More differences can be seen among categories. Information requirements associated with the *conduct* of operations tended to be

---

mation, "Network Centric Operations Conceptual Framework," *Network-Centric Operations,* Web site, n.d. As of June 11, 2007: www.oft.osd.mil/initiatives/ncw/ncw.cfm.

[3] Specifically, for timeliness, urgent is "1," time sensitive is "2," and not time sensitive is "3." For reliability, a "1" means the information has to be highly reliable; a "2" means that it should be evaluated for reliability by experts; and a "3" means only that the information should be pertinent. For security, "1" means that the information should be restricted to U.S. forces; a "2" means that it can also be shared with coalition forces; and a "3" means that it can be publicly distributed.

Table 2.1
Aggregate Assessments of Timeliness, Reliability, and Security

				Sourced from		
	Timeliness	Reliability	Security	Intelligence	Operators	Population
What to bring	2.4	1.9	2.4	2	1	5
Whom to trust	1.9	1.6	2.2	5	38	31
How to conduct	1.7	1.4	2.0	3	29	9
How to judge	1.8	1.9	2.3	2	11	2
Specific operations	1.8	1.7	2.1	1	10	9
When to leave	2.0	1.5	1.5		2	
Average total	1.8	1.6	2.2	13	91	56

NOTE: In some cases, two sources were indicated for a requirement, in which case, half a point was added to both sources and the results were summed.

quite stringent; those associated with broader assessments of the operational environment were considered less stringent for all dimensions.

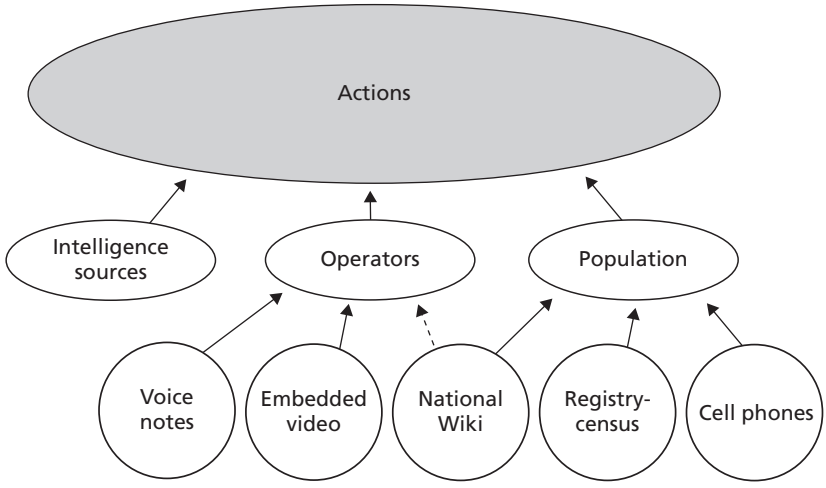
Reliability was judged as being most critical of the three characteristics; it is necessary if forces are to capitalize on the agility they should possess. In most cases, the information to satisfy these requirements had to be either highly reliable or at least vetted by experts. By contrast, security tends 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.

The 160 requirements can be classified by those that are primarily up to intelligence operatives to ferret, those that can be generated by operators in the course of their military or security duties, and those best provided by the citizenry themselves. Granting these imprecise, and somewhat overlapping categories, the numerical results, based on data in the Appendix, are still revealing: 90 can most naturally be supplied by operators; 57 come from the population, and only 13 require intelligence operatives. Note that these requirements are limited to the support of military operations and do not include the information useful for bolstering government legitimacy, distinguishing insurgents

and criminals from the population, or providing security services in general. The latter are largely derived from the citizenry. This reliance on the population suggests a need to rethink the application of the security rules that characterize normal military information systems to similar systems that support counterinsurgency (i.e., ICON). This goes double if U.S. operators are to work side by side with counterparts in civilian agencies and with coalition and, in particular, indigenous forces.

For these reasons, gathering information to counter insurgency requires its own framework and model, one that acknowledges the role of traditional intelligence collection but then goes beyond it. As Figure 2.1 illustrates, the information required for successful operations rests on three pillars, and each of these pillars, in turn relies on specific sources. The next four chapters offer some thoughts on how to accomplish the collection of this intelligence.

Figure 2.1
New Sources of Information



NOTE: Arrows with solid lines suggest primary conduits, while the arrow with the broken line suggests a secondary conduit.

RAND *MG595/1-2.1*

CHAPTER THREE

The Registry-Census

This is the first of four chapters on the sources of information. The first two—how to facilitate and carry out a registry-census of the population and cell phones—mostly deal with information on specific individuals. The next two—on embedded cameras and a national Wiki—also collect fine-grained information in which the actions or opinions of thousands, perhaps even millions, of people are highlighted. This stands in great contrast to the requirements of conventional warfare in which information of enemy forces is all important and information on local citizens, who are best advised to leave the scene, of much less value.

Why collect such information?

First, the geographic amalgamation of personal information can help better characterize the neighborhoods or villages that security forces happen to be operating in. This matters when carrying out operations such as sweeps, roadblocks, or arrests.

Second, the amalgamation of personal information helps in gaining the broader macro picture: How many people have been hurt or killed in the war; what kind of crimes are being committed; who is getting employment and where; and who is staying put or leaving the country? There is nothing like knowing the numbers to gauge progress or lack thereof—but only if the effort has been made to collect the numbers. Furthermore, if the process by which numbers are collected is transparent and visible (much as a census is), the numerical results provide more credibility for any argument that rests on such numbers. Such credibility may be contagious, making the case for arguments

based on facts other than numbers. Credibility, in turn, is essential to winning the psychological component of insurgency.

Third, information is the foundation of good governance, a pillar of legitimacy. Governance, here, means the provision of public services, whether security and safety services (e.g., an efficient 911 system) or social services (e.g., health care, education, and public assistance). Of course, there can be copious information on the public, which still does not offer much in the way of useful services; police states are one such example. But it is quite difficult to provide public services, much less do so efficiently, without knowing who the population needing services is. Third-world governments tend to have difficulties providing public services, but, armed with such information, they—not to mention the U.S. government—have less excuse for not knowing how well services are being delivered.

Fourth, such information provides a *start* in distinguishing the insurgents apt to hide within the population, from the rest of the population—or more broadly, to distinguish those willing to help from those eager to hurt. If you want information about the population as a whole and in its multitudinous aspects, there is no good substitute for going out and collecting it, one individual or household at a time.

Fifth, to be somewhat indelicate, information about individuals may be necessary to persuade each one to help the government rather than helping the insurgents. Insurgencies are defeated, in large part, by intelligence, much of which comes from the citizenry: e.g., witnesses to events or intelligence about who is affiliated with whom. Insurgents, in turn, want to know who is informing on *them* or at least who is cooperating or working with the government in general (many of those who died during the troubles in Northern Ireland were accused informants). Similarly, the ability of insurgents to find and threaten those who work for the Iraqi government or otherwise interact with American forces has multiplied the obstacles to countering insurgency there. Those uncommitted to either side should weigh the possibility that the act of informing or even interacting with one side may bring down the wrath of the other side. Both insurgents and authorities can potentially wield this power—although with potentially different procedures and consequences. The balance of coercion dictates the balance of intelligence. In

the long run, the government tilts the balance in its favor by removing the coercion that insurgents can wield, but in the short term, the consequences of *not* helping the government have to be comparable. The greatest incentive is the most precise one: if you inform (or support or etc.) you will be assuredly punished, and if you do not inform (or etc.) you will assuredly not be. Once the "assuredly" turns into "probably" or the "probably" turns into "possibly" the attractions of informing (or supporting, or etc.) relative to the fear of punishment go up (ditto for the converse: if ill-treatment is independent of activity, why not take hostile action against the authorities?). Precision and discrimination (as well as proportionality) promote the perception that authorities are legitimate, fair, and just. Such perceptions increase popular support for the government (or, in opposite circumstances, for insurgents), with the above benefits that flow there from. So, discrimination helps; discrimination, in turn, requires information of a most detailed sort.

Categorizing the Information

As Chapter Two discussed, there are few operations that cannot be improved by knowing something about the individuals that operators encounter.

Personal and Social Information

The most basic way to learn about the citizenry is to carry out a registry-census: registry in the sense that the government is taking and keeping names and a census in the sense that information about people and where they live is collected and merged into a database.[1] Both a registry and a census are required. A registry alone answers the who but not much about the what; a census answers the what but, without names, says little about the who.

---

[1] This is not a particularly novel idea. David Galula, *Counter-Insurgency Warfare: Theory and Practice* (New York, Praeger), 1964, p. 116, argued: "Control of the population begins obviously with a thorough census. Every inhabitant must be registered and given a foolproof identity card."

Five lines of information—basic census, relationship, buildings, employment, and health—form the core of the registry-census. The *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). In contrast to U.S. census data—which are tabulated, amalgamated, and kept private—these data are more akin to registration and will be used in their disaggregated state.

The *relationships* information covers family ties, notably relationships to those in different households—siblings, parents, and the extended family (and, thus, more than what the U.S. census asks for). In countries prone to insurgency, kinship ties tend to be a better predictor of political activity and affiliation then they are in the United States. A disproportionate number of terrorists are close relatives of other terrorists. Many Palestinian suicide bombers were closely related to victims of Israeli counterinsurgency operations.

The *health* information includes the mobility status of individuals (something that can often be ascertained by inspection—but not always, e.g., severe asthma or arthritis) and medical conditions that can benefit from state intervention, either routine health care (e.g., does this person need to be seen periodically?) or in emergencies (e.g., the record of ambulance visits). The first is useful in emergencies. The second one may be made available to social service personnel but also comes in useful if governments are to win public support through a vigorous program of social services and health care.

Work information is about who works where. It reveals the employment status of a person and, by aggregation, the economic status of a community. It can also serve as check on (or be served by) a census of establishments. Because people change jobs frequently, such data should be resurveyed periodically to stay current. Countries with social security systems collect such information automatically, but, in insurgent-prone countries, such systems may be the exception rather than the rule.

License information is inherently a government function and really should not have to be collected by census methods (after all, governments should know whom they are licensing). Drivers' licenses and

vehicle registrations are an obvious examples, but some countries may have others (e.g., use permits, hunting/fishing licenses, and machinery operation licenses). That noted, the records may be inadequate thanks to, for instance, indifferent, nonstandardized, or disconnected district offices or the destruction of records. If so, fresh surveys may be needed. Converting the record of licenses (which may be only in the form of paper files that may sit only in district offices) into a database will require work.

Systematic Incidents and Reportage Data

Incidents data and buildings data merit note, particularly for operations. Incidents data are, or should be, the province of security officials and their assistants, rather than census officials. Such incidents would range from visible crimes, to crime reports, and nonroutine contacts between citizens and authorities. What gets included need not be incidents as such—odd behavior may suffice. This amalgamation can be a quite valuable tool. COMPSTAT (computerized statistics), New York City's master compilation of crime reports, for instance, deserves a chunk of the credit for the city's falling crime rate in the 1990s. But such tools require effort; not only should district reports be amalgamated and standardized, but time and effort may be required to get all the data (who, what, when, where, how) filled in completely and correctly.

Many police departments (e.g., in Chicago or Los Angeles) make it a point for officers to make systematic notes of street behavior (especially when it may involve gangs). Officers receive a specific list of what to look for. Such notes are collected, processed into a database, and made available throughout the police department. Such a system has been adapted by Lockheed-Martin for the U.S. Marines in Anbar province, apparently to good effect. Incidents data will not arise spontaneously. When indigenous police are being trained, it may be useful to train them in keeping good records (and when they are at work, reinforce this) of the same sort that U.S. operators would.

Such practices should be systematized,[2] but with attention to some issues. First, the list of what to collect needs to be continually revised, keeping what proves useful and discarding what is of little value. In addition, what works will change as the environment and insurgent tactics change. Second, there needs to be an easy, nonobtrusive way of taking such notes; the next chapter, on cell phones, suggests how this could be done. Third, there has to be some sort of indexing or categorization method to find these comments; some obvious ones are by time and place, but it may also be useful to develop a simple standard taxonomy by which operators can bin such reports. This way they can be more easily collated and discovered. Fourth, reporting habits tend to flag if not sufficiently reinforced, thereby making databases increasingly obsolete and irrelevant. Attention to this issue coupled with appropriate incentives to keep up the flow of good information are warranted. At a minimum, operators should be able to see the aggregate results of their reporting efforts. Perhaps needless to add, if little benefit to the counterinsurgency results from collecting this information, the effort will cease, and this is just as well.

---

[2] Systematization means (1) accurately, honestly, and completely recording what was observed or what was talked about, (2) putting the record in an archive, (3) ensuring that every incident discusses what, when, where, and, if known, who, and (4) making the archives systematically available. Obstacles to good systematization should not be underestimated. People are not born with the habits of mind that lend them to respect the value of good data, and cultures vary in their ability to inculcate the requisite habits of honesty and diligence and the ability to make detailed observations. Setting standards high enough, educating officers, and giving them enough good people to emulate hardly hurts either. Military and other security patrols asked to acquire such habits may need convincing that what looks like tedium produces tangible value—but, of course, if their skepticism prevents such data from being collected in the first place, such indications may be hard to come by. On top of that, we can only guess at the pressures that may warp such reports: bribes, the pulls of friendship or clan membership, or the possibility that the presence of such activity reflects badly on security authorities. Victims may, themselves, be reluctant to come forward if they feel their efforts are futile, or worse, can put them in danger. Nevertheless, because it is difficult to imagine how to reduce the toll of incidents without such reporting, heavy emphasis by U.S. forces, perhaps leading by example, would not be wasted.

Buildings Data: The National CAD Model

Counterinsurgency, particularly in an urban setting, calls for three-dimensional maps, with the inside of buildings getting as much attention as the outside. In essence, operators need to see cities as they might be viewed by three-dimensional computer-aided design (CAD) programs.[3]

Such a model serves various purposes in urban operations. Only a three-dimensional model, for instance, can define lines of visibility and potential fields of sniper fire and, thus, denote safe or unsafe areas for urban combat or convoy operations. They also offer clues about where insurgents might plant improvised explosive devices (IEDs). When threats may be literally around the corner, it helps to understand at least what the terrain looks like in areas that cannot be directly seen. The inside of buildings are relevant when the buildings need to be entered during a pursuit or to take cover. Foreknowledge of a city's layout can help considerably in choosing among alternative routes of ingress or egress.

Developing a CAD model of a city rests on several sources. Surveillance platforms, both in space and in high altitude, are a sine qua non for constructing a two-dimensional baseline supplemented with topographic information, but they are not optimized to generate building shapes. They could be supplemented by lower-level unmanned aerial systems, especially in mapping out nooks and crannies. Because they are more likely to be controlled by ground-level operators (rather than the intelligence community) and because their technology is not particularly exotic, their products can be readily shared.

In countering insurgency, however, there is also a need to know the internals of buildings, as well as a fine sense of what they are used for. Many operations—such as conducting raids, cleaning out or guarding a building, or checking out suspicious objects within a building—require operating from room to room and are, thus, greatly helped by knowing how one room relates to another; the same holds for services such as firefighting or evacuating individuals. Even events that are nor-

[3] Although CAD programs were invented to facilitate *design,* the standards they support are equally adept at representing extant three-dimensional objects.

mally outside—such as a pursuit or crowd control—can become inside events if people dash into one or another entranceway.[4]

Thus, the CAD model should contain data on building internals: e.g., what the building is used for, how it is subdivided into units, the corridor layouts, occupancy patterns, and information on its construction. Perhaps needless to add, the latter information is difficult to collect from the outside (e.g., outer space) and requires that someone go into the building (or at least look at records from those who have). Such a survey can be carried out by local civil servants (e.g., fire and safety inspectors).

A three-dimensional model of a country and its cities may prove to be of immense benefit to users outside the security domain: from local government officials (e.g., fire and safety, city planning, and taxation) to institutions and individuals in the real estate, construction, and repair trades. It would seem, therefore, that opening this CAD model to everyone has merit. But how? On the one hand, there are very few individual facts in it that cannot be ascertained by anyone on the ground. On the other hand, the total corpus is of immense planning value even to insurgents. Thus, small leaks can be tolerated while large ones cannot be. The standard application of the mosaic principle[5] suggests, therefore, that the entire corpus be restricted to people with high clearances, but doing so would vitiate many of the benefits of the CAD model. A more reasonable approach would be to use something like Web hosting, with a downloadable interface module to make the CAD model accessible to planning or visualization tools. Explicit controls would be in place to flag and prevent wholesale downloads from the server, and audit tools would indicate patterns of inappropriate or suspicious usage.[6]

---

[4] Some urban operations (e.g., in Mogadishu and Hebron), by destroying walls, also succeed in exposing the inside of buildings to the outside.

[5] In other words, if the picture is sensitive then every tile in it needs to be classified.

[6] For example, it would be suspicious if someone repeatedly views some part of the city without having a legitimate interest in it. There are also privacy considerations that have to be protected to the extent that the CAD model holds data on building internals. The controls necessary to satisfy the various equities and interests may evolve to become quite sophisticated over time.

Getting the Information

Having established a rationale for detailed information on the country's citizens, how can correct data be efficiently collected without alienating the very population the authorities are trying to appeal to? Five lines of information—basic census, relationship, buildings, employment, and health—would have to actively collected, often one household at a time. Door-to-door census taking used to be routine in the United States and is still practiced whenever a mail-in form is lacking. Nevertheless, such a practice may be anything but routine during an insurgency.

There will be many problems with conducting a periodic census, but funding should not be among them. The developing world tends to be characterized by surplus labor and low wages. Going door-to-door to ask questions has to be considered an attractive job compared with alternatives. Even at $5 per hour, a generous wage in such places, if census takers could complete five households a day (also a generous measure), it would cost no more than $40 million to cover five million households (the total in Iraq or Afghanistan). Another army of clerks will be needed to process the information and ensure that it is complete (e.g., every building is accounted for) and at least somewhat consistent. Nevertheless, insofar as a good jobs program is important to a successful counterinsurgency campaign, it could be money well spent.

Another problem will be getting in the door in the first place. Many communities, even within the United States, do not wish to be counted—and the kind of counting at issue here is closer to a registration because the data are not made anonymous and the accuracy of each piece of information is at issue (in a numerical census, undercounts and overcounts may balance one another). The desire not to be counted is not entirely irrational; in the United States, it is based on the belief that undocumented immigrants, by being counted, would thereby become much more likely candidates for deportation. Similarly, in a country in which the fear of arbitrary arrest lingers, the notion, however mistaken, that the appearance of a census official correlates with subsequent detention may be understandable. This is not made easier by the

evident fact that the primary purpose of such a census-registration *is* to help the authorities.

Getting census takers in the door may, therefore, require a public education campaign that explicitly (and correctly) associates census takers with social service aspects of government and downplays the link to the security, and especially taxation, side of government. In some communities (and cultures), it may also help to dispense small tokens of appreciation.

Alas, even if citizens do not associate census takers with security services, this does not guarantee that the insurgents will not make that association, and they may, therefore, be of a mind to put such census takers in peril. If such risks arise, then census takers may have to be escorted by authorities, therefore, making any security disassociation far less credible. In the case of full-fledged insurgency, there may well be neighborhoods and villages where *no* government officials can venture at all (e.g., Fallujah in 2004 or Ramadi in 2006). Discretion may be the better course of valor. The consequences of postponing a census may be modest—irrespective of how well each resident is known by name, very few will be willing to tell the authorities very much until they, themselves, feel safer.

Error management is important. One precaution is to ask questions in ways that minimize incentives to lie.[7] Another precaution would be to include periodic revisits—these are, anyway, required to stay current on changes in employment, residence, and health. A related technique is to have different visits for different parameters (e.g., one census taker asks about relatives, while another asks about building internals). Different visits that reveal incompatible information are a red flag that

[7] Iraq's 2003 official census by the Ministries of Trade and Planning (and thus, presumably, taken under Saddam Hussein's regime) revealed that the population was 58 percent Sunni and 40 percent Shia; see Focus on Advocacy & Advancement of International Relations, LLC, "Iraq's 2003 Official Census by Ministries of Trade and Planning for the Food Coupon Distribution for the UN Oil-for-Food Program" (Washington D.C., 2003). As of June 11, 2007: http://web.archive.org/web/20040615113507/http://www.faair.org/images/Iraq-Census-Total-2003.pdf. If recent reports are accurate, a third of the Shia felt it in their interest to be counted as Sunni.

may require additional visits and, more important, may cast doubt on one of the census takers.

Information Reliability and Timeliness

The importance of data reliability is derived from how it is used. Small random errors, for instance, will not greatly affect the quality of aggregate data (e.g., a neighborhood's unemployment rate). In other contexts (e.g., noting seven siblings when there are only five), errors, at worst, cast doubt on the fastidiousness of government employees. Then there are the graver mistakes: mistaken ascription that results in someone's detention or, worse, the wrong address is produced for a firefight or a shut-in was not evacuated because his or her existence was never recorded. Common sense should prevail: If errors have grave consequences, double checking is in order; cross-correlating data for internal consistency and reasonableness is useful and relatively inexpensive if done in moderation; the same is true for "flowing back" new data (e.g., someone's death) into all affected databases. If data are computerized, they need to be protected against tampering and archived to permit recovery if such protections fail. Finally, inculcating respect for high-quality data among those who generate, manipulate, or depend on it is a good idea.

Obsolescence can be limited by prompt recording and frequent updates. But its prevalence varies. Some data, such as an individual's birthplace, never change. Only birth and death affect blood relationships. Incidents data reports get older but do not go out of date. The timeliness of license data depends in large part on how long licenses last; this information, in effect, updates itself when licenses are renewed. How buildings are used tends to change faster than a building's layout, which, in turn, changes faster than its foundation structure. Conversely, employment and address data can change frequently, especially for the young. The government either needs an underlying mechanism (e.g., a tax withholding system) that generates information in the course of events or a specific mechanism to resurvey individuals. In a sense, a registry-census is as much a process as a product.

Can the data also be protected from leakage? Limitations on how many records can be accessed at one time and carefully auditing all downloads are probably good procedures. Yet, some moderation is in order. First, census-type information on an individual is normally insufficient, on its own, to get someone in trouble with either insurgents or government. Since the aim is to facilitate a great many operations, to be really useful, there has to be a lot of data transferred. Second, it would be ultimately counterproductive to withhold such data from the indigenous government while, at the same time, counting on the government, itself, to collect them.

Toward a National Identification System?

The general purpose of the census-registry is positive in that it represents the data foundation for helping individuals so counted. The purpose of a national identification system, however, is to detect those who wish to evade the grasp of authorities, of whom insurgents would be a critical subset. If identity cards have to be presented at certain times and places, insurgents would have to acquire them, allowing them to be tracked, or avoid them and, thus, avoid checkpoints, lest they be exposed as suspicious when so encountered. By contrast to a census, universality results, not from the application of grunt work, but from disincentives to being excluded. This disincentive applies to foreigners 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.

Hence, there are three conventional rationales for a national identity system: universal, consistent identification; the profiling of individuals; and the ability to spot those outside the system. Technology allows possibly one more: the ability to recognize people on the street.

National identification systems are, in a sense, as old as paper, but as with so many aspects of life, they are poised to be transformed by ubiquitous cheap electronics: the "new" U.S. passport with its

machine-readable radio-frequency identification device (RFID) is just one harbinger.[8] Normally, most developing countries prone to insurgency would not have a sophisticated system within their scope. But any nation that has the skills to outfit and maintain a modern information system should find that the hardware is little barrier; if not cheap enough this year, the year will soon arrive when it is.

The issue in this chapter is not so much whether a national identification system can add to the government's information superiority in countering insurgency (where there is general agreement), or even whether, on net, it is a good or bad idea (about which there is considerable disagreement),[9] our concern is simpler: Can a plausibly workable system be designed?

To address this question, we discuss issues associated with citizen registration, acquiring their identities at checkpoints, and the more difficult challenge of acquiring identities without or away from checkpoints.

Registration

For a national identification card registration system to be protected against subversion by insurgents, (1) it should be difficult for anyone to concoct a new card except by going through a registration process and (2) the material collected as part of the registration process should be largely accurate.

---

[8] An RFID is a small electronic device that responds to a specific radio signal with an identification number (and, in some cases, additional information). These devices started showing up in corporate identification cards in the mid-1990s and are now being considered for merchandise.

[9] The U.S. Marine Corps, *The Small Wars Manual* (Washington, D.C.: U.S. Government Printing Office, 1940, p. 25) argues:

> Another advantage of such government is the authority to require natives to carry identification cards on their persons constantly. It has been found that the average native is not only willing and anxious but proud to carry some paper signed by a military authority to show that he is recognized. The satisfaction of this psychological peculiarity and, what is more important or practical, its exploitation to facilitate the identification of natives is[sic] a consideration of importance.

Cards need photographs and a set of hard biometrics, such as fingerprints. A facial photograph is part of the process by which after-the-fact fraud can be detected, and it helps individuals pick out their card from among others.[10] If the national identification system is linked to the use of cell phones, then getting a voiceprint should be part of a registration process, too (see the next chapter for why). Fingerprints make it very difficult for someone to have two identification cards with two different names (or, what is equivalent, appear twice in the registration database with two identities). Either a face to facial-photograph comparison or the more precise finger-to-fingerprint comparison will indicate that the holder of the identification card is the rightful owner.

Such cards should be electronically readable for both record keeping and fraud resistance. Assuming an uncorrupted registration process, every card could have embedded with it a digitally signed byte string composed of the photograph, the identification name or number, and perhaps some details about what day and in what office the individual was registered. Since it is characteristic of a digital signature that it is virtually impossible to generate it correctly without a private key, any card that is displayed as a purported ID card[11] will fail to

---

[10] Names, by contrast, may be problematic. It is hard to think of a card anywhere in the world that does not include a name, but recent events in Iraq suggest that the ability to read the name off a card has its drawbacks—to wit, insurgents can also demand to see them. Since a person's name is a good clue, in that country, to whether the individual is Sunni or Shia, many Iraqis have acquired a second ID card to indicate ethnic solidarity with whomever is asking at the point of a gun (so, a Sunni handing out the alternative card would appear to have a Shia name and vice versa). Insisting that a name be on the card *and* that the card be spoof proof may put people in jeopardy. Even if names give no clue to ethnic identity, why allow insurgents or anyone else for that matter to collect any such information? An identification card without a name forces people to read it electronically, which means that it is possible for the government to control where a card is read, especially if the information is encrypted. It remains only to control the distribution of decryption devices.

[11] Despite the repeated references to "cards," in a well-networked nation, it is possible to have a national ID system without the card. By keying an ID number or pressing a thumbprint to a platen, for instance, an access device could generate a call to a master database that indicates whether the person is registered and, if necessary, returns a picture for visual comparison. For the sort of countries prone to insurgencies, networks are often sparse, and so this would not work everywhere. Hence, the need for a card.

compute correctly[12] if it has not been issued through the registration process—unless it is an exact copy of an existing identification card. But if so, the only people who could get away with carrying such an ID card would be those who looked close enough[13] to the individual whose card it was. A person can duplicate his or her own card, but the only conceivable purpose for doing so would be to give someone who looks very much like him or her an identification card for which he or she otherwise would be ineligible. If the card also has a digitally signed byte string to represent the picture taken during registration, finding someone who could pass as a match would be hopelessly daunting.

A national identification system tends to work best when everyone above a certain age in the country has a card. As a practical matter, this means that foreigners should also possess one as well—a matter, for first-time visitors, of taking a passport (accepting its data as real) plus a fingerprint and automatically creating such a card. Taking fingerprints on the spot is actually easy; the US VISIT program does it for millions of visitors a year.[14] The procedure adds less than a minute to the entry process (producing a card for a first-time visitor may add a few more minutes).

Although, in most cases, the name under which people register themselves is their real name, the exceptions tend to be the individuals of greatest interest. Even if the name is right, the claim for citizenship[15] may not be. In this case, therefore, asking for an ID card may not find

---

[12] Any attempt to alter the byte string that represents the digital photograph (or other information) will generate an error when fed, together with the signature byte string, into a validation algorithm.

[13] The validating process also has to be able to read the visible picture electronically and confirm that it comports to its digital representation. Otherwise someone could substitute his or her own picture on the identification card while the old digitized picture is used in the validation algorithm.

[14] Currently, it applies to all visitors coming in by air from countries that do not participate in the visa-waiver program—which is to say, the less-affluent ones.

[15] Conversely, such a distinction may be important only in countries that find themselves in the uncomfortable position of being a magnet for others (as the United States is vis-à-vis the developing world). Most foreigners are not insurgents, and rarely are insurgents more than a minority of foreigners.

the kind of outsiders for whom the authorities are looking. Developing countries generally do not have the same breadth of documentation that a U.S. citizen may be used to needing: e.g., a birth certificate; income tax records, which require a Social Security number from a child as young as two; vaccination records; a driver's license, or school yearbooks. Where such documentation does exist, it is easier to fake for not having been archived: e.g., there would be one birth certificate in the files for every birth certificate in the hand and stored for easy electronic retrieval. Unless someone who is claiming citizenship once registered (e.g., with fingerprints) as a visitor on an earlier day, it is nearly impossible to prove someone is not a citizen. Where data are anyway incomplete, absence of confirming data is not very good proof that the basis for the data does not exist. The least problematic way to proceed may be to ask people about where they were raised (perhaps asking for a description in some detail) and who their relatives are. Some replies may raise eyebrows and can be challenged on the spot; others will reveal inconsistencies with the registry-census. In practical terms, the government may have little choice but to issue identification cards with the proviso that they are subject to revocation should the testimony fail to be corroborated.

Acquiring Identities at Checkpoints

Although registration, in and of itself, provides many of the same benefits of a census but is somewhat better authenticated, it would strike owners of ID cards as more than a little absurd if no one ever asked for them.

Checkpoints, by definition, are locations where ID cards may be read and recorded as such. The most obvious place to put a checkpoint is at the national border, where such things almost always exist anyhow. An electronic ID, however, offers the advantage of being able to record someone's passage instantly and, one hopes, correctly. The amalgamation of such information can establish patterns of goings and comings. If someone's name comes up as needing attention, analysis of border crossings can establish whether he or she is inside or outside the country (assuming he or she crossed the border legally).

In general, checkpoints can be categorized as permanent, standing, or spot. A military base or national border may be set up with a permanent checkpoint to include everyone who enters. A standing checkpoint might be a street barrier put up in emergencies to log people who pass through. A spot checkpoint, as the name suggests, is likely to be carried out by, say, local police desirous to see who is in the neighborhood.[16] If there are standing checkpoints, all of them require card-reading devices that are transportable, and portable ones are needed for spot checkpoints.

Checkpoints could serve two purposes. One is to find those who are not registered or whose registration has been revoked (e.g., because they gave false information during the registration process). The latter population is apt to possess a fair percentage of people in whom the government has an interest (plus a fair percentage of procrastinators or those whose registration contained forgivable errors). Two is to log the passage of those who are registered. Such information, when amalgamated, could be used to build profiles of such individuals (to be sure, a yet uncertain art) and may also help with forensics if violence erupts in areas associated with these checkpoints.

Although some checkpoints may be used to deny entry (e.g., into a government building) or to seek undesirables for detention, they should be the exception. The broad purpose is to keep track of the population. Those with identification cards would be registered as such; those without may be photographed or fingerprinted so that they may later be matched with the identity of a particular individual.

Acquiring Identities Without Checkpoints

The problem with relying on checkpoints is that their presence is no surprise. They may be useful in keeping suspicious folks from walking into sensitive areas such as government buildings (albeit less good at keeping such folk from storming such areas). But it is difficult to see a thinking insurgent, or anyone else wishing to evade the attention

[16] Spot checkpoints may, however, be problematic from both a force protection and civil society standpoint; in contrast to fixed checkpoints, they may appear to be fishing expeditions.

of authorities, willingly running through a checkpoint (although they may get caught up in it).

If the aim is to catch insurgents or at least identify people who may be (and know they are) suspicious, then spontaneous ID checking would have much to recommend it. As long as the card-reading devices are sufficiently portable, it is quite feasible to have authorities swoop in and give everyone the once-over. This process will survey a fair sampling of the population, especially if the area is precordoned. Unfortunately, this is not the sort of activity that will endear the authorities to the population, and it is difficult to imagine any outfit but the most aggressive repeating the process very often. It also requires that people be mandated to carry their ID cards with them every time they step outside their houses—another government-imposed hassle.

The real trick would be to determine who is who without having to bother them terribly much. In other words, how can people's ID cards be polled remotely? One way to do this would be to place RFIDs within the ID cards. As RFIDs, they can be remotely polled: e.g., a strong radio wave would be broadcast and all the ID cards in the area would chirp their unique code back—but there are many practical problems that would have to be addressed, and it is not clear that they can be.[17]

In normal circumstances, people are best polled as a street-wise cop might do: recognize those he knows from long experience and

[17] The trick is knowing whose RFID beeped. Individuals could funnel through narrow portals that limit the number that an RFID reader system would have to view at any one time, but this is scarcely different from a checkpoint. Checking RFIDs on the street presents more problems. First, most RFIDs are intended to be used in close proximity to the reader. Use at a distance can be challenging, in part because power and receiver antenna requirements might make the readers fairly large; user mobility adds complexity. Second, if the reader has to detect not only the signal but know where it is coming from, the technology gets that much more complicated and more difficult to use. Otherwise, it would be hard to know whose ID is whose—or which person does not have an ID at all. Third, validating the ID requires matching the face on the ID (which may be accessed by calling up from a database a picture associated with an ID number) to a person who is often looking elsewhere. Some of these objections go away if the polling is done by walking past people. Yet, the bulkiness of the reader required to poll the RFID plus the constant need bring up from the network (with its usual latency) pictures of faces associated with the ID numbers acquired and compare them with the actual faces of people walking past make for a serious operational challenge.

take the names of those he does not—and, if in no other cases, these IDs can come in handy. Unfortunately such police officers are not so easy to come by in normal times, and insurgencies are hardly even normal[18]—which means that most of these officers may be newcomers. Rapid population movements (especially into cities as a result of a rural insurgency) that create the need for most police newcomers also make it difficult to pick out who does not belong.

Might it be possible to scan a face and determine who it is (in most cases) or determine that no firm identification can be made with any face in the database and therefore ask for an ID card? Here, the goal would be to recognize most people. The less often an ID card has to be asked for the less hassle is involved all around.

Unfortunately, today's face recognition technology is not good enough to identify an individual on sight alone if this person could be one of several million. Technology may not be the problem—it is unclear that human faces are sufficiently stable from one minute to the next to permit sufficiently reliability even with perfect technology. But most of us are not in random locations most of the time. We live somewhere specific, work somewhere specific, have particular habits, frequent certain markets, have certain friends, and so on. Among people standing in front of a specific store in a particular town, chances are good that most of them will have shopped in that store before. A high percentage of people even in so public a place as a train station are prior frequenters. Within a group measured in the thousands or perhaps even tens of thousands, face recognition (coupled with cueing information on sex and age) should be a good deal more reliable. A picture could be taken by forces equipped with a high-quality phone camera and relayed together with the picture's coordinates to a database. Computer matching, as noted above, would be able to identify which of the, say, several thousand possible people, the individual is.[19] Knowing

---

[18] Policemen have become particularly favorite targets of insurgents in Iraq. See Michael R. Gordon, "Wary Iraqis Are Recruited as Policemen," *New York Times* (July 24, 2006), p. A1.

[19] If people hang out in groups, the job is easier: e.g., the person on the left could be one of three people, and the person on the right could be one of five people but only one of the three people is friends with one of the five people, so it is probably the intersecting person.

people's habits and associates means that the problem of picking them out among millions is reduced to the easier problem of picking them out among thousands.

The better the automatic technology, the more that asking for a card would be the exception, thereby saving manpower and making the identity-checking regime less obtrusive.

An important secondary purpose is to make it difficult for irregular forces to venture into areas where they are likely to be spotted by cameras (which can then run some form of identification check on them) and to make them be particularly wary of getting within eyesight of authorities. The effort to avoid getting caught comes at the cost of operational agility. Outside of small-town or tight-neighborhood conditions that allow individuals to know who is a stranger, the hope is that technology in the hands of competent forces can allow what are, in effect, official strangers (authorities from elsewhere) to provide a similar quality if not quantity of assurance. But this technology would need work in the first place.

Conclusions

Detailed knowledge of the neighborhoods and villages where war fighters are operating is not only possible but invaluable in knowing the local leverage points and how best to harvest the vast intelligence that they contain. An insurgency that can threaten with any credibility individuals who collaborate with the government or the United States must perforce have a great deal of information on who is doing what. For the government's part, although census and incident data are only a start in applying countervailing pressure, they are democratic (quiet people are counted as thoroughly as noisy ones), and they can serve as a foundation for later, more detailed efforts to prepare the counterinsurgency battlefield intelligently.

The challenge for the U.S. government is persuading other governments to conduct a registry-census when such duties have not been otherwise assumed. At the very least, the U.S. government should create the expectation that such a registry-census is a sine qua non for effec-

tive governance, absent which our assistance may be a wasted effort. The hardware and software required to conduct a registry-census is readily available, although the indigenous government may need financial support to acquire them in requisite quantities; the same holds for training. The only technological challenges here are those associated with the electronic ID card; how to do them is known, but reliability, consistency, and correctness in a country in the midst of a counterinsurgency have to be assured. Face recognition technology, especially if coupled with algorithms that cue off likelihood-of-appearance measures, may, however, need further research and development to permit the standoff identification of people who do not belong.

CHAPTER FOUR

A Well-Wired Country

The ability to control the cell phone switch—and through it, the cell phone system—can be a tool of singular power in the search for information superiority. To demonstrate as much, this chapter outlines a systems concept of cell phone switch control and user registration, illustrates how such control can be used to facilitate counterinsurgency operations, and addresses issues associated with making the system work in the interest of the government.

If, as noted, insurgencies are about individuals who choose to align with or oppose the constituted government in greater or lesser degree, then information about individuals at a fine-grain level is central to countering insurgency. To know how people are moving and interacting on a day-to-day basis, there is no information quite as rich as that which 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 lasts. If the cell phone system, however, is not architected to deliver such information, the net result may be not only to throw out such information, but, ironically, to level the information field, when the extant preponderance of resources (notably U.S.-supplied resources) should otherwise be favoring authorities.

Iraq illustrates as much. When U.S. troops liberated Iraq in 2003, the country proper[1] had zero cell phones. Within three and a

[1] There was a 50,000-phone system in the part of Kurdistan not under Saddam Hussein's control.

half years, there were seven million cells phones, or one for every two adults. The now-evident desire of Iraqis to own cell phones could have been used by the United States to dramatically tilt the information battlefield in its favor. This did not happen. Contracts for private cell phone service were let; the U.S. government (as far as is known) kept its hands off; and, apart from whatever back doors (if any) have been secretly put into the switches, the cell phone system has been neutral in this war. Insurgents and noninsurgents alike have equal access to it. Indeed, because insurgents start with little infrastructure of their own, their access to cell phones has been a far greater boon to them than to counterinsurgency forces. Because prepaid cards allow cell phones to be used by anonymous callers, there is no good way to know with any degree of confidence who is calling whom.

Systems Concept

As a general rule, more-advanced technologies show up and proliferate first in developed countries before they enter developing countries. After all, advanced technologies tend to be expensive; they require an educated populace to use them and a sophisticated infrastructure to support them. Accordingly, automobile ownership in developing nations today is similar to what characterized the United States in the first quarter of the 20th century.

Cell phones have been a conspicuous exception to this trend, largely because they do not display the three inhibiting features. First, cell phones are basically nothing but electronic chips covered in plastic and have, thus, experienced the same sharply falling cost-performance ratios that benefit all electronics. Second, it is immediately obvious how to use a cell phone's basic features. Third, ironically, whereas cell phones *do* need an infrastructure, such infrastructure is substantially cheaper and easier to install than what is needed for landline phone service. The world will, therefore, soon see its second billionth cell phone customer—equivalent to half of the world's adults.

This trend forms the background for the basic tenets of the systems concept:

- Encourage and accelerate cell phone usage,

but

- Shape the cell phone environment in ways that favor authorities.
- Ensure that cell phone calls can be associated with registered users.
- Ensure that 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.

We discuss each basic tenet in turn.

Encourage Cell Phone Use

Cell phone users are powerful networked sensors. The phones themselves provide information on their callers. Callers can provide voice and, increasingly, video data on events. As networked sensors gain recognition as a powerful component of modern warfare, the logic of proliferating them needs little repetition.

As noted, policies to accelerate cell phone usage are like pushing on an open door (indeed, in some cases, the problem will be to accommodate rapid increases). Nevertheless, faster is better, and universal is best.

If we assume private provision of cell phone service for reasons of efficiency and innovation, then government's job would be to facilitate the building out of infrastructure and encourage pricing plans that accelerate user growth. Favorable policies may include ready access to spectrum (although unused 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 airborne transmission towers. Direct subsidies for switches, or at least guaranteed or reduced-rate loans for their acquisition, are another option.

The first step in encouraging cell phone usage is to make cell phone handsets available at, or somewhat below, the marginal cost of producing a handset at the factory.[2] This prospect is only modestly complicated by the special features, explained below, that cell phones would be required to have and the low likelihood that handsets can be subsidized by high monthly service charges. One approach may be to make a mass initial purchase (e.g., in the millions of units) as a way of keeping prices reasonable. A similar proposal for a basic cell phone intended for use in Africa persuaded one company to offer phones for $50 each if purchased in bulk.[3]

Shape the Cell Phone Environment

Everything important about a cell phone system stems from its software—what goes into the handset[4] and, more important, what goes into the switch (e.g., features that determine which calls are routed or which information is retained).

It is important that the U.S. government[5] be able to control this software, either by retaining the ability to write the necessary modules

---

[2] There is a practical lower limit on pricing associated with the risk that phones sold too cheaply will be purchased for gray-market sales overseas.

[3] It is important not to confuse the cost of a cell phone with the price that people pay for it. Many subscriber plans toss in a "free" cell phone as part of the contract, with the expectation that what the consumer pays over the life of the contract (or through the invocation of early-withdrawal fees) will more than cover the cost of the phone itself.

[4] Note that although these features should be built into the phone upon distribution, cell phone software can be easily updated wirelessly. Expect this to occur frequently early on as experience on what works and what does not work is gained and exploited.

[5] Or the indigenous government; the case for the U.S. government lies in the possibility, discussed below, that it may want to pull the plug on the system if the indigenous government uses it to create a police state.

and seeing to their insertion in the overall code base,[6] or by developing specifications that tell the cell-phone operator what the software needs to do.[7] Some of these specifications follow logically from the aforementioned security requirements (that all cell phones be reliably associated with a unique individual) or geospatial requirements (that all cell phones communicate their position). Others will be developed through learning which features work better than others. In essence, the U.S. government would "own" the switch—not in the sense of its being government property, but in the sense in which a computer hacker would use the term—the ability to make the switch do what the U.S. government wants it to do.

It is important, for instance, that government requirements inform the handset "environment"—what the user sees when the phone is turned on and what is invoked with each menu selection. Most of this environment will be dictated by commercial considerations and strongly influenced by what consumers want—but it can be tilted one way or the other. Nevertheless, it is important that it be biased correctly. For instance, calls to authorities, including but not limited to 911-like calls, should be easy to make (e.g., the number would occupy a more prominent spot on menus, would occupy a spot on menus that are easier to reach, or would allow the user to call them up with fewer keystrokes). The same would hold, albeit with less priority, for phone calls to nonemergency services. Such privileged access, however, can be more broadly extended. Nongovernment groups that do or would support the government (e.g., friendly mosques) can have phone numbers built into the menu, to be accessed and to deliver services, such as sermons of the day. These features would not only make it more attractive

---

6 This means that someone has to have enough information on the code base to insert such modules without harming the rest of the cell phone system's functionality.

7 This is not a perfect substitute for writing the module code. Without knowing the overall system code, it may be unclear which specifications are easy to implement and which are not. Furthermore, adding another link in the chain creates opportunities for time-delaying negotiations and forces the government to undertake testing to determine whether the cell phone company really did as promised and whether the specifications are, in fact, met by the code to the government's (rather than the phone company's) satisfaction.

for such groups to support the government, but those that do would see their power increase over those that do not.

Phones might also be designed so that citizens can build their own calling groups, some of which might serve as neighborhood self-defense. For instance, with only a few keystrokes, it might be possible to pull updated lists of all members' phone numbers or send mass messages out to the group.[8]

Pricing is a key part of the environment, especially if monthly billing is hard to collect and so every call is charged separately. Therefore, just as calls to authorities are easy to make, they should also be free, even if the call is used to transfer pictures (the cell phone as sensor). Another useful pricing feature would be to reduce the cost of calls made to friends and family, at least at the outset. This feature might not only encourage the proliferation of cell phone use, it could also give authorities a first-order guess as to what social networks look like.[9]

Associate Cell Phones with Registered Users

When most cell phone users are subscribers, it is relatively simple to determine who is calling whom. In developing countries, particularly those wracked by insurgency, monthly billing is hard, and, therefore, service tends to be paid for with each call. People typically do this by purchasing stored-value cards and running down their value with each call.[10] Such cards retain the user's anonymity.[11] but such anonymity frustrates intelligence collection. If cell phones offer no clue to who is using them, insurgents have no reason to avoid them.

---

[8] In such cases, it may be better to keep such lists in the switch rather than in individuals' handsets, lest loss of a cell phone to insurgents reveal many people at once.

[9] This feature could be offered within limits or at a modest per-friend cost. If everyone in the village is labeled as a "friend," not only will all calls be sold at a discount, but no one will be able to infer a meaningful social network from this service.

[10] An alternative to using a stored-value card is to store the value in some part of the phone itself with the value being refreshed by electronic contact with a value-dispensing device.

[11] However, every phone emits a distinct electronic signature, but if we cannot infer whose phone is whose by calling records, initial purchase, or by usage patterns, such information is not very useful.

One solution to the anonymity problem is to require that phones carry the equivalent of the subscriber information module (SIM) chips that are routine parts of today's cell phones. In this case, however, each SIM would be associated with a particular individual and would be issued only in person. SIM data would be broadcast by the calling cell phone and the receiving cell phone, as part of the digital "handshake" that allows a call to be placed. If the switch does not read a SIM as part of the call setup[12] on either end (of a cell phone to cell phone connection) the call will not go through and the relevant handset or handsets will be so notified.

Just as the SIM would be comparable[13] to a national identification card, the SIM registration process would likewise be similar: People would come to an office, provide some evidence of identity, sign some papers, get photographed, and provide a hard biometric, such as a fingerprint. Foreigners who want to use their cell phone in the country would do the same, adding information from their passports to indicate their status. If there is a national identification card in addition to a SIM cell phone, then the two registration processes would be combined.

The problem of false cell phone identity is also similar to that of the national identification card. In many ways, associating identity tokens with cell phone services bolsters both. The combination of photographs, calling patterns, and whatever transactions and contacts

---

[12] There are ways to encrypt the call setup information (using the SIM to obtain the exact time, perhaps location, and a private digital key) so as to prevent SIMs from being intercepted and echoed in ways that spoof the cell phone switch into thinking that someone else is making the call. Encrypting in this manner is not trivial and is one more thing that may go wrong. Thus, whether to institute such a practice depends on whether spoofing is a serious problem.

[13] If the SIM chip *were* the national identification card, it would have to be simultaneously small enough to fit easily into a phone but large enough to contain an easily viewed picture: an inch-square picture could be a "sweet spot." If phones are thus ID cards, they may be able to use a technology (e.g., RFIDs) that permits reading without contact. People could wave their phones at a reader rather than pop the SIM card out and push it back in every time an identification card needs to be shown. Pictures on the SIM card would have to be visible when the SIM is in the slot—a feature that, because it is not common elsewhere, may raise costs.

have taken place under the fraudulent identities will be used to make educated guesses about callers. Again, as with national identity cards, the registration process does require registrars to be resistant to dishonesty, corruption, bribery, threats, or insurgent sympathies. Depending on particular circumstances, therefore, registration might be better carried out by government authorities or by employees of the phone company.

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. The former yields accuracy to within hundreds of meters in an urban area and a few kilometers in a rural one; GPS is accurate to 20 meters everywhere. E911 capabilities are mandatory in new U.S. phones, proof that the technology is available and not particularly expensive. That noted, GPS signals tend to be somewhat weaker than phone signals, and there will be circumstances (e.g., on trains) when phones can report their position approximately vis-à-vis transmission towers but not more precisely vis-à-vis GPS.

The point is to deliver such information to the switch, much as GPS-based information is delivered to E911 desks in emergencies. At a minimum, therefore, cell phone locations for both sender and receiver would be transmitted when calls are attempted (whether or not they are connected) and perhaps periodically during the course of the phone call. In addition, because cell phones, when on, are continually searching for cell towers, they can also be equipped to broadcast their GPS-based location during such "chirps." If we wish to go further and acquire the location of phones when they are *not* on, that too can be arranged by programming them to turn themselves on periodically, broadcast their position, and then go back to sleep—albeit at a cost to battery life.

Using the System's Capabilities

Experience in receiving, analyzing, and using the data will reveal surprises: both new ways to use the data and new forms of data to use. It may take years for such a system to assume a stable configuration in the face of the learning that should and will go on. Even if it does nothing else, 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.

Government Services

Although most of what it takes to provide security for an individual is to provide it for the entire community, enough of it is personalized to make it worthwhile to invest in a warning and protection system that can make citizens bond with their government.

The proliferation of cell phones facilitates E911 services. If these cell phones come with cameras that allow evidence to be gathered on the spot, assistance is all the more ready to act on arrival. A cell phone system could also issue warnings of dangerous neighborhoods either via alert (that is, when someone enters the neighborhood) or through the equivalent of e-commerce: An inquiry to a crime center when coupled with GPS information can return a neighborhood-specific set of tips and warnings.

Perhaps needless to add, if such an E911 or incidents-based tips-and-warnings system is to emerge from the phone system, it is necessary that there be a security system behind it. People will not bother to dial 911 if no one comes running. Hence, an important element of government services is the ability of the authorities to determine whether their subordinates are, in fact, responding to calls: Are they consistent, do they put the right amount of manpower onto the case, do they favor certain neighborhoods over others? The cell phones will hold the answers—they provide a basic "green-force-tracker" system, which will indicate whether officers are going to places where they should as well as avoiding places where they should not go.

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 easily reported. If a call is made while the incident is still in progress, the cell phone will give authorities the location (an improvement in accuracy and precision over callers trying to determine where they themselves are). Phones with built-in cameras can send pictures of the area to authorities, which will assist in sizing up the situation, collecting evidence of what happened and who was responsible, and even identifying possible insurgents (many of whom linger in the neighborhood of incidents).

The GPS capabilities of the phone offer another palpable advantage—they make it difficult for cell phone users to credibly deny that they were on the scene. Thus, following an incident in a particular area, authorities can readily determine at least some of the phone owners in the area at the time.[14] Then authorities can call these people, who have little choice but to either describe what they saw and heard or come up with a plausible reason why they saw and heard nothing.

This example, incidentally, illustrates two recurrent themes about any intelligence: the need to take action on it and the dangers of doing so. A capability to respond more smartly to any incident is of little value if the will or capability to respond at all is weak. Conversely, if the incident is an insurgent ploy, the ability to flood an area after the event may play into insurgents' hands (sometimes, terrorist explosions come in pairs: the first to draw in responders and the second to exploit the then target-rich environment).

Actionable Intelligence

Summed over each individual, a cell phone user's comings, goings, and calls, when amalgamated, paint a detailed picture of his or her life. The ability to know where people have been, for instance, is a major

[14] The accuracy and completeness of the information depend on how frequently cell phones broadcast their position, a rate that may be engineered to differ if cell phones are in use (needing to constantly search for the location), if they are on (periodically finding the location), or if they are off (not needing to know the location but may, as argued, be engineered to do so anyway).

clue to whom they associate with and what they do with their time. Bear in mind that, apart from winning popular respect, the most difficult challenge in counterinsurgency is to distinguish friend from foe. A record of phone calls is by no means conclusive evidence, but it is a start. If such phone calls are consistent, with appearances in insurgent strongholds when there is no reason for presence there, then a more in-depth look may be advisable. Conversely, if there is already intelligence marking an individual as a person of interest, a pattern of calls may be further proof. Alternatively, cell phone–related intelligence may help to establish that someone does *not* merit further scrutiny. This type of intelligence may help counter a recurrent problem in Iraq, where those who bear a grudge often finger that person as an insurgent so as to get them in grave trouble with the authorities.

Summed over a neighborhood, the data present a living tableau of its energy flow, an indicator of how well the neighborhood is doing and who is occupying it. In addition, the system provides other benefits: clues to the social networks of phone-toting individuals (the "friends-and-family" program) and a bias in favor of neighborhood self-defense and government-friendly institutions.

Patterns of cell phone usage can also be mined as part of "traffic" analysis. A rise in calls that suddenly terminate in a suspicious location, for instance, could be a clue to an impending operation. The unexpected deepening of quiet in a neighborhood may be a clue that the residents are evacuating, also an indicator of trouble (and, yes, someone on the scene could ascertain that more easily, but letting a computer raise the alarms saves on having to maintain a presence in any of thousands of neighborhoods simultaneously). Comings and goings at suspected insurgent hangouts can be used to determine if such locations are, in fact, what they are suspected to be. Patterns of interaction between suspected insurgent recruiters and people who later prove to have been recruits can be analyzed to determine who, in fact, was doing the recruitment.

For example, if our troops are engaged in an operation in a neighborhood or village, the information on each person's location can be converted and displayed as a flow of gray dots. Such displays can help avoid civilian casualties or help authorities infer, for instance, whether

people are scattering to avoid the movement of insurgents. Imagine, for instance, how West Side Story might have ended differently if Officer Krupke could have learned, by monitoring the movement of dots representing cell phone movements, that the Jets and the Sharks were moving toward a rumble. (And even if he arrived after they scattered, there may well have been subsequent cell phone traces used for forensic analysis.)

Still, whoever wants to make use of these data should be prepared to invest a considerable sum in additional networks (to haul the data from the switches to where they can be fused and analyzed), storage for the data, and, most of all, analysts and software to comb through the data for patterns.

Other Uses

As noted, the cell phone system can be designed to make it easy to form groups and, more to the point, mobilize them for action. An unfettered cell phone system will not care whether the groups are progovernment or proinsurgent—but one that favors the government may make a difference in two ways. First, it can give favored groups a space on the cell phone's menu, either as part of the original software or by broadcasting small changes in software and thereby putting it on the menu when necessary. Such groups can be the seed for a rapidly burgeoning activity. Second, by linking phones to individuals, it should be possible to see "flash mobs" organize themselves in real time, and thus authorities can intervene to protect order and nip the mob in the bud. Such phones also provide a trail of intelligence for after-the-fact analysis.

Clearly, owning the cell phone switch can be helpful in forensics and postevent analysis, in large part because insurgents will not always be careful about not taking their cell phones out on operations. One who plans on placing an IED by the side of the road in the dead of night would face a difficult choice. He could venture out without communications and, thus, be limited in his ability to react to events (e.g., the unexpected presence of police). Or he could venture out (perhaps forgetfully) with a cell phone, which would periodically announce its location, thereby, alerting authorities to its anomalous appearance late at night by the side of the road. Even if authorities do not determine

that such an appearance is noteworthy at the time, if the IED were planted and subsequently detonated, they would have a short list of people to talk to as suspects.

The last hypothetical example in this subsection involves roadblocks established as checkpoints. The government may, in some cases, announce such roadblocks "up the street" by flashing a text message to cell phones in the vicinity to give people in their vehicles time to prepare for inspection. Those who got the message and turned away could be detected by the pattern of their cell phone traces. Not all such people will be suspicious in interesting ways (some may want to avoid a traffic jam or may have forgotten their driver's license), but all of them may merit more surveillance as a result.

Our list of examples could be multiplied. Clearly, though, it demonstrates the enormous potential of this system to aid in countering insurgency *if the appropriate analytic and response capabilities are in place,* which create the value added.

The Cell Phone Network as the Primary Counterinsurgency Communications System

A solid, reliable cell phone infrastructure can also permit cell phones to be used as the *primary* communications device for U.S. and indigenous operators. Since both are using the same system—indeed the same system used by everyone in the country—interoperability issues will 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.

To be sure, U.S. forces already have connectivity—of a bulk sort. To those familiar with communications in the everyday world of the American metropolis, the equipment with which U.S. counterinsurgency operators go to work is astoundingly primitive. Individual foot soldiers have zero real-time connectivity; squadrons have SINGGARS (the single-channel ground and airborne radio system), a 40-pound box with data rates comparable to early 1990s-era phone modems. Perhaps these limited communications represent the state-of-the-art in battle-

fields in the middle of nowhere, but counterinsurgency is fought where the people are, and where enough people of sufficient means gather, communications links follow.

Because the features of modern cell phones are converging with those of palmtops, a cell phone can provide data connectivity in easy-to-use forms. Such connectivity can provide a window into useful databases, such as the counterinsurgency equivalent of incidents reports or wants-and-warrants reports. Furthermore, it would not be difficult to reprogram cell phones to facilitate the entry of reports into the phone in text or preformatted form (such as those described in Chapter Eight).[15] Such reports would be relatively straightforward to amalgamate and process for database use (also, anything that comes over the cell phone switch would be automatically stamped by time, place, and person).

Cell phones have two well-understood disadvantages relative to military communications systems. First, connectivity cannot be guaranteed. The handset may not survive environmental or combat stresses or the cell towers may be victims of combat. Because we cannot predict cell phone availability, 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 in case that service is available? Units can then decide, based on the particular circumstances of time and place, whether they want to carry military communications gear as a backup.

Second, normal civilian cell phones transmit in the clear and can, thus, be intercepted (as cell phone calls routinely are). There are two approaches to that problem. Operators can learn to exercise communication security, which they should do anyway. Or phones can be engineered to permit automatic encryption using the National Institute

[15] Recording such reports using voice and then converting them to text, either automatically or through third-party services, may overcome the reluctance of operators to spend time on paperwork. It would also permit events to be logged soon after they happen, rather than at the end of the day, thereby lessening the tax on memory. That noted, automatic speech-to-text programs are in their gawky adolescent phase in English and much farther behind when it comes to other languages. Furthermore, such programs do noticeably less well in noisy outdoor environments.

of Standards and Technology's advanced encryption standard (AES).[16] Such phones need not meet National Security Agency standards—insurgents are unlikely to have the code-breaking skills that intelligence agencies of large countries do, and whatever operators say would rapidly lose its military value over the time required to decrypt it, even by the most sophisticated code breaker. Some high-end cell phones already come equipped with AES-enabled communications hiding the internals, but not the externals, of calls.

Neither of these disadvantages provides any real reason not to pass out cell phones routinely both to U.S. forces and, if necessitated by economics, to indigenous forces.

Issues

Although owning the cell phone switch as a way to gain information superiority has a lot going for it, making it work right raises quite a number of issues:

- Secret surveillance
- Insurgent responses
- Lost or stolen SIMs
- Spoofing GPS signals
- Commercial considerations
- Follow-on phases
- Avoiding a permanent police state.

[16] The most straightforward way to do this would be for the cell phone, when asked to place an encrypted phone call, to pass each party a one-time AES-standard (hence symmetric) cryptographic key (itself encrypted using the asymmetric private key of the handset). Each handset would have circuitry that would digitize the voice (which it does anyway) and use the key to encrypt the digitized voice stream, whereupon the receiving phone would decrypt the message and then convert it into an analog waveform. If it is also desirable to hide who the parties are, then the phones would also have to encrypt the call setup information using the private key of the cell phone switch.

Secret Surveillance?

Many of the features of the system—such as the linkage between the SIM and the individual—will be obvious. Other features, such as the ability to gather call setup information, are easily guessed. People may even guess the use of GPS tracking. Even those without cell phones may find themselves wondering how authorities can suddenly find certain people so quickly.

Thus, the better course of wisdom may lie in letting people know exactly what the system is doing (although the degree of U.S. government intervention in setting up the system need not be trumpeted). Indeed, the public understanding of the system's features may be crucial to their intelligently using such features for demanding security services.

The one capability not yet mentioned is content interception. Whoever owns a cell phone switch can engineer it to intercept content. Indeed, cell phone content fly through the air and can thus be intercepted by anyone with the right equipment, whether or not the phone company approves. Undoubtedly, some individuals will have their content intercepted—but that does not imply that the system should routinely collect *all* conversations. The obstacles to doing such collections well are enormous. First, collecting all conversations requires an enormous amount of resources, not least of which is storage; moving it out of the host country and back into the United States for analysis and safekeeping would tax even the bandwidth of the sturdiest fiber-optic lines. Second, searching all the material for telltale conversations is daunting. The National Security Agency is said to use keyword search for starters, but keyword-based flagging depends on the existence of speech recognition algorithms in the native language of the target country. Third, the challenges only multiply if insurgents employ encryption or even simple indirection and codes (such as the hijackers' using "the Faculty of Law" to refer to the Capitol). Fourth, it is too tempting to pay attention to internals at the expense of attending to the harvesting of externals, which are rich enough as it is. Nevertheless, if insurgents assume that their calls are constantly being monitored, the difficulties they have to go through to communicate surreptitiously will be multiplied.

If people know that cell phones can be used as tracking devices, will they use the system anyway? Probably—and for the following reasons.

First, the strong link between cells phones and government security services may make such phones more attractive. There is a thin line between "the government is watching me" and the "government is watching over me," and a system that can evoke the latter may be appreciated for that reason.

Second, this relationship is likely to be emphasized if the insurgency, itself, makes people less secure. The current difficulties of the Iraqi government in establishing itself have less to do with how repressive it is (although Iraq's interior ministry has employed serious killers) and more to do with how weak it has appeared in stopping insurgents.

Third, if users are given the option to broadcast their location more widely, they may find themselves benefiting from *m-commerce,* location-based services that rely on intercepting cell phone location signals to promote themselves and their wares.

Fourth, even if people object to the government's tracking them, their desire to own cell phones may be so strong as to overcome such objections—especially when there is no other cell phone coverage available. In Mumbai, which is, on average, a very poor city, 40 percent of the population has cell phones. In war-buffeted Sierra Leone, a cell phone entrepreneur set up shop and earn his investment back in a year. Even in anarchic Mogadishu, cell phone entrepreneurs prosper (despite 40 percent of their costs being consumed by "security" forces).

Insurgent Responses

When insurgents get as much or more use out of the cell phone system than the government (let alone U.S. forces), they pretty much let the system stand and rarely hassle people just because they carry cell phones. It is naïve to expect them to ignore the fact that the cell phone system is deliberately tilted against them, and there are many ways they could react. Indeed, insurgents have attacked cell phone towers in Iraq (especially in Anbar province) as cell phones are increasingly implicated in the capture of high-value insurgent targets.

Insurgents could, of course, avoid making cell phone calls completely, and to some extent, such a reaction should be expected (e.g., Osama bin Laden stopped making satellite calls after being informed circa 1998 that they were being intercepted). This could be counted as a victory even if we assume that insurgents had the discipline and the communications security to go off the air completely. Not only would abjuring cell phone use impair their command-and-control capabilities, it would get in the way of their ability to reach out to third parties one on one.

It is more likely that they would try to use cell phones anyhow. Insurgent membership is rarely strict. Affiliation can range from leadership to full-time fighters, part-time fighters, supporters of various grades and hues, and the broader mass of sympathizers. Asking all of them to avoid cell phone use when everyone else feels free to use them may be asking a great deal. Some may use cell phones to help recruit new insurgents or mobilize sympathizers in support of an operation. Since insurgents, especially urban insurgents, are rarely self-sufficient in material or infrastructure, they may use cell phones to supply themselves. If an insurgent group has a political front (as Sinn Fein was for the Irish Republican Army), it might feel free to call across such a military-political "wall." The more insurgents are tempted to use cell phones in ancillary ways, the more they will leave telltale traces, which alert authorities can use to weave an intelligence web. Insurgents may use cutouts to place calls, but if these cutouts are identified and apprehended, they may be more forthcoming than the more dedicated insurgents. Furthermore, to be in a position to use cell phones at all, some insurgents, or those close to them, have to register, again, giving authorities a start in figuring out who the insurgents are.

Insurgents might try alternative means of communications.[17] In Iraq, some have used Thuraya's satellite-based phones. Such service may support the central leadership, but it is no good substitute for a cell phone. The service is far more expensive than terrestrial cell phones, and the equipment is expensive, bulky, and inconvenient to use. If a local government, facing this situation, chooses to make such telephony illegal, then possession of the equipment would be prima facie risky. Whether or not the United States could persuade satellite operators to limit the footprint of their satellites over the insurgent country is unclear; because footprints have fuzzy boundaries, service cannot be provided everywhere on one side of the border and nowhere on the other.

Landline phones are another alternative, until they fall under similar rules as those discussed below; in any case, there goes the mobility. Or insurgents could try a cordless to landline link (some cordless phones tether out to as much as a mile). Doing so would at least make it uncertain exactly where the caller is, but knowing the owner of the landline would offer a hint as to who was making a call, and it would not prevent content interception.[18]

Sophisticated insurgents might try a solution that uses Wi-Fi to connect to a computer via voice-over IP (Internet protocol). Even if every computer had to be registered to use the Internet in the same way that cell phones are, insurgents could try to hitch a ride on a system that was running Wi-Fi wide open. Banning Wi-Fi computers would

---

[17] International calls provide a critical loophole. Although it would be possible to trace the location and identity of someone within the country on one end of the call, corresponding information about the other end may be limited to the phone number; a lot depends on what the foreign phone company is allowed to know and convey. It is theoretically possible that two domestic callers could converse undetected if they call each other through a foreign country. If this turns out to be more than a theoretical notion, one response would be to make an exception to normal practice and listen to the internals of such calls (which would be a small percentage of all cell phone calls). Listening to content would also permit detection of an international node being used as a junction point for a domestic call.

[18] Several companies are coming out with phones that act cordless when near a landline and act cellular when not. Phones that require that individual SIMs be in place before they work are practical and may be useful in many situations, but they would not make a lot of sense in such environments as businesses, in which phones are routinely used by many people.

be next to impossible (it will soon become impossible to buy a laptop that does not have Wi-Fi built in); banning its use or forcing people to use access controls would also be quite problematic. However, if insurgents are forced to cruise city streets trying to "war dial" with their laptop looking for an open connection in order to communicate at all, then one might as well declare victory at that point.

Insurgents could try to set up their own cell phone system instead or, if sufficiently clever with engineering, try to establish their own point-to-point radio network. These solutions can work well only in terrain they physically control. Otherwise, the emissions from such a setup would be a dead giveaway in the face of U.S. signals intelligence assets.

Finally, insurgents might give up trying to communicate with cell phones and attempt to reduce everyone else to the same common denominator by targeting the cell phone system itself. Whether they do so directly (by attacking cell phone towers) or indirectly (by threatening those who carry cell phones), such a policy will hardly endear them to a population that is either already dependent on its cell phones or that would dearly love to be. Insurgents may try this tactic anyway. Fortunately, point infrastructures, such as cell phone towers, are generally easier to defend or at least harden than landline infrastructures. Furthermore, in the face of a threat, such towers can be placed with sufficient redundancy so that it would take many simultaneous attacks before service was interrupted in more than spots—and cell phone towers, as noted, can be emulated by aerostats flying beyond the reach of insurgents.

Lost or Stolen SIMs

Insurgents could steal other people's phones—technically their SIMs, since the phones themselves are interchangeable—and make phone

calls that way. A call would go through, and the theft victim might be held responsible for the mischief associated with that phone call (e.g., an IED placement). If the use of phony SIMs is pervasive enough, the credibility of the entire system can be jeopardized.

We outline two approaches to addressing this problem: (1) binary and (2) analog. Neither, though, is foolproof, and misidentification will be a lingering problem in any system.

The binary approach is to determine, with more or less fidelity, that the wrong person is using the phone/SIM. Part of the approach is to hold the phone owner responsible for what happens with his phone (much as soldiers in the Israeli Army are held strictly accountable for their guns). Such accountability would give owners a strong incentive[19] to report lost or stolen phones—if they realize that they are missing and if they are alive, conscious, and not being held hostage (none of which can be assumed during insurgencies). Then alerts could be set for phones, or they can be shut off.

These are, of course, a lot of ifs. In the case of cutouts, especially those with clean records who then make themselves scarce, a standing threat to trace calls back to the original SIM owner may not suffice to keep top-level insurgent friends from using their cell phones. So, other approaches are needed.

One approach is to issue a personal identification number (PIN) for every registered user. Phone calls attempted without the right PIN would not go through; several bad tries in succession would result in phone service being cut off until the owner returns the phone/SIM to the phone store. This measure is relatively simple, but it adds hassle to every phone call—PINs can be forgotten, a PIN requirement is one more thing that can go wrong, it does not protect against conniving or extorting PIN numbers from people. A cutout may let others use his

[19] People misplace and think they have lost phones all the time. Given the risks of losing one to an insurgent coupled with the hassle of getting phone service turned off and back on when the phone is found (which may entail a visit to a registration office), it might be useful to provide an electronic device matched to the SIM that makes it easy for people to contact the phone system and disable their SIM temporarily while its status is being determined. If the phone is recovered, the same device can reactivate the phone.

phone, and the phones can still be used for receiving calls (unless PINs are also required at that step—a larger hassle).

A second approach is to require a fingerprint[20] match between the individual and the phone in order to make or receive phone calls. This step eliminates the memory problem and prevents cutouts from using the phone (but it also keeps friends and family from using it as well—unless they happen to be carrying around their own SIM chip). It, too, is one more thing that can go wrong (e.g., fingerprint platens have to be kept clean), and it does add some cost to the handset. How much cost may depend on how rapidly such devices appear in the commercial world, notably for laptops.

A third approach is to require some match between the voice on the line and a voiceprint taken at the time of registration. This method does not add anything to the cost of the phone (no extra hardware is required and the software resides in the system), but it will raise the time and cost of registration. The real problem is that validation may be time-consuming and may fail frequently—emotional stress, colds, and ambient noise all introduce error. Nevertheless, even if voiceprints are not used as call locks, they may be worth gathering as part of the SIM registration process for reasons discussed below.

If the more deterministic measures are infeasible, some probabilistic methods might exist to suggest that a given SIM is probably not being used by the individual to whom it was registered. If the original owner, for instance, had established one calling pattern and then lost his or her phone, which results in a different calling pattern, that changed pattern could trigger an inquiry (e.g., a request to bring in the SIM). If only the SIM was stolen and attached to a new phone, that change, in and of itself, would also be suspicious (every cell phone has a unique electronic signature). Similarly, if a keystroke pattern or a voice pattern can be inferred from initial phone calls (this requires that the owner has used the phone long enough) and this pattern suddenly changes, then this deviation may be indicative that the phone has changed hands. Or if a voiceprint is taken at registration (see above),

[20] Requiring a "warm" fingerprint match (bearing in mind that these phones are used in war zones) offers more protection but adds to the cost of the phone sensor.

then running voice-comparison algorithms on *all* subsequent calls may indicate—after a cumulative degree of mismatch (to average out stress, colds, and background noise)—that such a phone was probably not being used by its registered owner. If fraud is determined, service would be cut off, and the owner would have to return to the SIM store to receive a new phone.

Additionally, the system can be occasionally spoofed and yet still be worthwhile. For example, using a cutout is not cost free. An apprehended cutout may provide access to higher-up insurgents. Finally, many of the advantages of the system, as noted, do not depend on insurgents not using cell phones—but it is better if they not do so freely.

Spoofing GPS Signals

A user may attempt to mask or spoof the GPS signal because it provides clues to where the owner is situated. To be sure, there are limits to how much help spoofing will provide—*some* location data are necessary to make phone calls, after all. Also, masking GPS merely enlarges the uncertainty over where the caller is; it does not make him invisible. Nevertheless, there are steps that can be taken to reduce the temptation to use masking and spoofing—e.g., tamper-resistant seals to prevent masking GPS signals and refusal of the switch to carry calls for which the GPS signals are inconsistent with those from transmission towers. Going further and refusing to connect calls that are not accompanied by GPS signals risk the phone being unusable in many locations and generally more frequently unstable (since GPS then becomes one more thing that can go wrong). An alternative is to look for patterns that suggest systematic concealment or malfunction, and, then, when the level of certainty passes some threshold, shut down service after informing the customer that his handset needs work.

Commercial Considerations

Even though a license to offer cell phone service is generally a license to print money, this proposal is more likely to drain rather than supplement U.S. government coffers. For instance, the subsidies used to accelerate cell phone proliferation could represent a major cost (although

puny in comparison to the overall cost of military operations in Iraq and Afghanistan). The first switch that comports to the standards described above is likely to be an expensive reworking of some commercial switch. Similarly, the first such system to be installed is likely to have nontrivial system-integration costs. As experience with such systems is gained (or as other countries adopt similar systems for their own use), costs should normalize.

One concern is the cost of handsets, but it is easy to overstate this concern. Consider its many desiderata. SIMs are already is use today, although cryptographically secure SIMs are not. GPS is already in the latest version of U.S. cell phones. Over-the-air software updates are also common in the United States. Stored-value cards and stored-value cell phones are common (at least overseas). Finally, an internal timer to wake up cell phones and to chirp their position is not common but does not appear terribly hard to make. Integrating all these features into one phone, however, may be a new problem to solve—and, while not inherently hard, it may still make such phones unique and, thus, more costly.

We have assumed that such a phone system will be privately provided. To be sure, the U.S. government could, in fact, establish such a phone system on its own, but governments have not been conspicuously successful in this business; entrepreneurs have. Thus, while, say, the Defense Information Systems Agency has the engineering skills to succeed, it would be asking a great deal to expect it to have the marketing skills or the agility to succeed as well—the same would be true for the large aerospace contractors. Left to their own devices, entrepreneurs would not set up a phone system that meets the above requirements.

Thus, coming up with a cell phone system that is inexpensive and flexible, yet does everything the U.S. government would want of it, would require (1) establishing a clean set of necessary requirements that still preserves enough room for favorable economics and service

offerings; (2) finding entrepreneurs (including established companies) who are willing to work with governments, who meet such requirements, and who can tolerate a certain degree of price regulation; and (3) perhaps toughest of all, devise a set of mechanisms to ensure that such requirements are met without making the system impossible to run and repair. Realistically, there is likely to be tension in the first few years while such entrepreneurs, the U.S. government, and the host nation government figure out how to work together.

But what if there is already a thriving cell phone industry in place? The amount of resistance there will be to meeting such requirements will depend on the institutional arrangements already in place: e.g., is the vendor a monopolist, does the vendor have other markets,[21] how politically connected the phone companies are with the country's government, to what extent are the phone companies free of ties to insurgents? Needless to say, established players will make their best guess about what their future would look like subsequent to a U.S. intervention in the wake of an insurgency. Everything after that will be about who has to pay whom off and for how much.

Others—notably the host government and cell phone users—also have to be persuaded. Convincing the host government is a matter of making the following points: (1) removing obstacles to information superiority is a condition of U.S. entry and "owning" the cell phone system is a key element of that strategy; (2) the United States will bear the cost of changing over the phone system, which will lead to (3) a phone system that is more widely used and available in more places, (4) with capabilities that any government would want to see in place, and, therefore, leaving behind (5) a cell phone system that may be more advanced than anything in the third world or the first world, for that matter.

Last will be the consumers. What would persuade customers to give up their existing cell phones—apart from the obvious fact that

---

[21] Any phone company that inserts location-surveillance equipment into its switches and handsets has to think about what that might do to its reputation in other countries. This concern is more than notional; the largest cell phone operator in the Middle East, Egypt's Orascom Telecom Holdings, has franchises throughout the region.

the old handsets will cease working after some point? A more persuasive case would include the following: the new phones will come with better services (including, see below, some Internet capability), not least of which is access to better security; the pricing will be more advantageous; and, to boot, it may even be a niftier phone (with cool games). In addition, a real world business, Apple, is betting on music and video capabilities to persuade customers to consider switching to the phones introduced in June 2007. Although only time will tell if this strategy works, there are successful precedents aplenty of merged devices (e.g., camera cell phones and upmarket Sony Walkmans).

Follow-On Phases

A follow-on phase is optional in that it is not required for garnering the benefits of the new cell phones.

The benefits of moving landline phones to "registered service" are primarily to frustrate attempts by insurgents to evade cell phone surveillance. Nevertheless, because landlines are largely immobile, their location is known (give or take the range of cordless phones) as is their ownership. Landline phones are often used by multiple people, especially in business establishments. Conversely, requiring a SIM card to use a phone may be a hassle. Except in residences with only one caller (in which case, the SIM card would already be in the phone), all users would have to carry their handsets with them or, worse, carry SIM cards to pop into and out of phones. If the latter, callers would have to go to the trouble of fishing it out, inserting it correctly, and then making a call, which, if there are additional security features, may require entering a PIN or a thumbprint. Doing all this while the phone is ringing is even more daunting. It may be simply easier to convert all landline handsets to registered SIM-based cell phones.

Making the Internet a registered service is both more challenging and more important—after all, the very anonymity of the Internet is what has made it so popular with terrorists. If cellular telephones were made attractive for Internet use, then the demand to use the Internet via landlines would be reduced (and surfing habits would be more available for inspection). Thus, a robust text-messaging capacity (à la short message service or instant messaging) may be attractive if priced reasonably (which is to say, a lot lower than the cost of calls). Although cell phones have not yet proven to be popular Web-surfing platforms, there is no technical reason why a cell phone cannot download music (or prayers)—there already is a surprisingly lively business in ring tones. Several companies are in the business of offering users cell phones that can play videos. Nevertheless, adapting popular Web sites so that they can be satisfactorily accessed from a cell phone will be a major challenge.

Making cell phones capable of accessing the Internet, therefore, will not on its own persuade people to abandon the personal computer as a device for accessing it.[22] To rope *all* Internet users into the same corral would require that the national ISP(s)—Internet service provider(s)—somehow require SIMs for log-in (or eliminate ISPs entirely). Unfortunately, that method "leaks" in many ways. Various methods can be developed to hijack someone else's Internet session. They include social engineering (e.g., taking over someone's seat at a cybercafé) to neglectfully insecure Wi-Fi connections (see above), and expectedly insecure wireless personal areas networks (such as via Bluetooth connections).[23] Worse, it is very difficult to interpret what a link between a user and a Web site really means (many jihadist Web sites are

[22] The tradeoff between wired and wireless access may depend on how far advanced technologies such as WiMax become and the extent to which they are competitive with fixed-site Internet access at, say, Internet cafés. Using cell phones as wireless modems creates a potential link between a person, his IP address, and his location.

[23] Note that this list does not discuss computer hacking—under the assumption that the linkage between Web site and user is made while the byte stream is still being carried over an individual physical line and, thus, before it hits the router. The assignment is made between the SIM card and the physical line and between the physical line and the accessed site. As such, it is not "hackable" in the normal meaning of the term.

actually "squatting" on relatively benign domains). If the accessed site is, say, a Hotmail account, then it would require the cooperation of the site owner to determine who is sending what mail to whom—but all that will be revealed is a user screen name, rather than someone's true identity.

For these reasons, while a strategy to migrate as much landline and Internet traffic through cell phones may reduce the mostly anonymous connection space, it will not eliminate it. Making SIMs mandatory on landlines and on the Internet may prove, in the end, to be too clumsy to achieve.

Avoiding a Permanent Police State

The cell phone system suggested in this monograph can provide a highly useful technical and operational capability for a nation under siege from insurgents, but it can also be misused to foster a 21st-century version of a police state. The technology itself is neutral, but it offers great potential for misuse. Once installed, it is likely to become integrated into the society.

Although how such a system is used remains the responsibility the host government, the United States cannot avoid the onus of being the supplier of the technology and operational expertise. Hence the question: How can we minimize potential damage from misuse of the technology, while also obtaining the benefits necessary to wage a 21st-century counterinsurgency?[24]

The United States has four types of tools to address concerns over misuse:

- Limitations on system transfer
- Policy implementations
- Operational procedures
- Technical options for decreasing the utility of the system.

---

[24] This question makes two assumptions. One is that the state possession of personal information, by making it easier to run a police state, thereby makes such a state more likely; the counterargument is that police states arise for other reasons and that having personal information only makes such a state less arbitrary in its repression. Two is that the United States, which may have invested the lives of its own troops to support the government, can nevertheless turn its back on that government when convinced it is becoming a police state.

The best option mix will depend on both U.S. and host nation sensitivities. In some cases, U.S. preferences for privacy protection may lead to more restrictions than locals would like; at other times, the reverse may be true. The reason for taking both viewpoints into account is that the very legitimacy of the counterinsurgency operation will be hurt if either side begins to see uses of the system that lie outside the pale. An upset U.S. public may withdraw support from the whole counterinsurgency effort, not just those aspects associated with privacy abuse. Conversely, if local sensitivities are trampled by the system, the indigenous government may lose precious legitimacy. After all, what constitutes privacy is dependent on the culture and circumstances. In most of Asia, the expectations for privacy have been to date far lower than those in the United States. In Europe, national governments and the European Union severely restrict the private collection of personal data compared with U.S. practice, while at the same time the national governments are granted freer rein than the U.S. government in terms of accessing information. National ID cards are anathema to many U.S. citizens, but they are common elsewhere in the world.[25] In religious Muslim countries, biometrics such as fingerprints and photographs may be quite controversial; in others, privacy protection against search and seizure might be quite lax.

Attitudes toward privacy are also influenced by civil conditions: the greater the perceived threat to personal security, the more willing people are to sacrifice personal privacy to regain security. Unfortunately, emergency measures during periods of peril risk becoming the new status quo. Thus, the erosion of privacy can easily become a permanent feature even for governments that start off quite benign. For less savory governments, the problem is worse, and the tools of security can readily be turned into the tools of oppression that continue to be used long after the emergency has ended.

---

[25] Witness the legislative contortions inherent in the Real ID Act of 2005, which attempts to make drivers' licenses into de facto national ID cards. Independent of the efficacy of the Real ID Act itself in boosting security, the level of opposition to this effort reflects a fundamental distrust of federal government power that goes to the core of U.S. politics.

This chapter and the one before it present two elements that may raise privacy concerns. One is a national identity card that includes biometrics and entails a careful registration process. The other is a cell phone system with a strong association between handsets and individuals and the ability to track the location of handsets.[26]

What follows, although not a complete examination of these issues, serves to suggest the care that should be taken in deploying such powerful technologies in support of a nation. Like the genie, once released, it is difficult to put back in the bottle.

Limitations on System Transfer. This option is about not allowing certain military systems to fall into the wrong hands. Unfortunately, there are limits to what the United States can do when friendly governments have an uneven track record in human rights by Western standards but need to be supported if the counterinsurgency is to succeed. In practice, this support tends to mean that as long as certain activities, defined as *red lines,* are not crossed by the host government, that government is eligible for certain classes of weapons; other red lines govern access to law enforcement assistance.

ICON, though, does not fall neatly into either the military or the police assistance category, particularly since the capabilities envisioned are similar to capabilities that already exist, at least in latent form, is every cell phone system. Even without the specialized elements of the system, the bulk of the more intrusive effort is technically feasible. What would be missing are the development of concepts of operation as well as training personnel to use the system to the fullest extent.

Among the various options, transfer restrictions are by far the easiest to implement. More so, a system that is never installed cannot be abused. Conversely, it is entirely possible that the indigenous government would abjure the system anyway if it makes its own operations more transparent or eliminates certain avenues of corruption (e.g., because cell phone systems are big moneymakers everywhere in the third world). Its installation may be more in the U.S. interest than in the parochial interest of the indigenous government. Denial is also

---

[26] To reiterate, the system is not designed to intercept content, something that is already easy to do with cell phone calls and is routinely done from afar.

a blunt instrument of control. It may, thus, easily not only prevent transfer of a system with many of the public safety features of ICON, it could stop almost all transfer of modern wireless communications systems. Furthermore, denial does nothing to help mitigate possible damage once the decision to deploy the system has been made, and the U.S. moves on. It is then that other types of safeguards come into play.

Policy Implementations. After deployment, usage policies provide another approach to managing the risks of misuse. The fundamental goal is to write clear lines within bureaucracies, and to the outside world, on how the system is being used. This approach falls into our general preference for enhancing effective governance as a way of increasing legitimacy of the host government. Formal policies, as such, demonstrate a government's commitments in building a safe, secure, and open society.

Some policies that might help are creating independent oversight, akin to independent police review boards, to develop formal criteria for determining when such tracking capabilities should be terminated; establishing formal guidelines on who can be tracked and for what purpose; and developing auditing policies that can associate individuals with specific system abuses.

Operational Procedures. Operationally, the most important aspects of the system will be a mix of control policies and techniques to enforce such policies. The operational procedures of the system are likely to make it more cumbersome to use but are a small price to pay to maintain citizen confidence in the system.

Controlling and maintaining awareness of where and how the data flow are extremely important. Use of a central repository for the data greatly simplifies monitoring of activities and makes the system easier to secure against physical threat. All data streams from that repository (to other systems or to human inspection) would be carefully logged for audit (which, itself, implies a commensurate security regime to know who is accessing the data). Such controls would both identify who has accessed what information and would make certain information, notably conversation content, difficult to acquire without going through specified procedures. Such procedures may include

judicial warrants or other third-party formalities. This approach separates the guardians of the data from the users of the data. It may be implemented by placing physical control of the system in the hands of someone other than a user—as long as that individual is not under the government's control and is sincere about preventing data misuse. Despite inevitable leaks, it is a time-tested way of guarding the guardians. For this reason, it should be enthusiastically supported by the host government as a way of knowing that its own security forces are not using the data for self-serving ends.

Another practical approach to preventing the host country from misusing the system is for the United States to manage the system itself and maintain control of important aspects of the system. If the switch (and handset) software, the analysis packages, and the call-setup and call-location data were held exclusively by the U.S. government, its ability to cripple aspects of the program would provide a near-term solution. Over the longer term, the benefits would be more modest—largely because it is the information produced, and not the system per se, that is of value to the local government, and over the longer term, many of the capabilities of the system can be reconstituted.

Holding the software but letting the data flow to the host government would give it a treasure trove of information on its own citizens, especially if one assumes it runs the SIM registration process. The host government may not be able to add further to this information after the plug on the cell phone monitoring capabilities is pulled, but it may have enough to target and even blackmail individuals. If the citizenry conclude, not unreasonably, that a record of their prior comings and goings implies that the state can track them henceforth, U.S. statements that these features have been disabled may be disregarded. Thus, the repressive effect may linger for years. In any of the cases in which the U.S. increases its control over the system, the United States will likely be held more responsible than if it operated at arm's length vis-à-vis the host nation. Given the poor prospects of effectively controlling

the system to exclude any misuse of information, there seems to be significant downsides to too much U.S. intervention.[27]

Finally, if the system is deliberately designed to be turned over to the host government for "mopping up" insurgents, the United States has pretty much given up on having any leverage whatsoever. Yet, must the software be transferred to the host government? Services such as system maintenance, troubleshooting, very large-scale database management, voice-based access authentication, social network analysis, and contact-based profiling are likely to remain partially in the hands of Western firms for years.

Technical Options for Decreasing the Utility of the System. Technical controls can also help as long as it is made clear beforehand about whether such controls are meant to be hard walls to prevent abuse of the system or speed bumps to retard and regulate inappropriate use. Hard walls tend to be difficult to build without resorting to nonstandard hardware and software, which are both expensive and difficult to support. If, instead, the goal is to shape the behavior of the host government, technical elements of the system are attractive, including ensuring that the code that routes the data is authenticated and that all potential back doors into the system are closed.

Again, central repositories help as does increasing the difficulty and cost of duplicating the system's capabilities elsewhere. More help could come from techniques to prevent the electronic transfer of information from the repository to any open network (and, thus, to the ICON described in Chapter Seven), thereby hobbling large-scale file transfers. The approach here is to prevent copying of datasets, while permitting queries into the database in secure and traceable ways. While ICON stresses sharing of data, this does not require that sensitive data be put on the open network. Architecting a system that maintains a series of protective gateways (see Figure 7.1 in Chapter Seven) to assure proper access to the most sensitive data will be critical for the success of the system. It may also be wise in some circumstances to allow the system to release such information in response to only certain

[27] The citizenry might also strongly oppose a foreign, rather than their own, government controlling this sort of system.

types of preset queries, thereby limiting most "fishing" expeditions. Such protection might be designed to have limited geographic, temporal, and personal scope (how many degrees can you follow a lead) without proper authorization.

Data security (perhaps via encryption) should also be part of the overall security package. The use of strong encryption of data will prevent some classes of problems, but it will not solve all of them.

A Note of Caution

In the end, however, and despite the best safeguards, the host government will come away from the experience with the wherewithal to engineer a police state should it choose to do so—which only further emphasizes the importance of inculcating proper political values upon U.S. entry and exercising great care in providing a "full-up" system to other countries. If nothing else, the host country will get the existence proof of such a system and an understanding what it can be used for, as well as some sense of what it takes to build and run it. Should it decide to pick up the pieces and rebuild the system following the U.S. departure, it starts with a ready infrastructure of hardware, including switches, towers, and handsets already distributed. There are also many clever third parties that could help reverse engineer such a system (although, in all likelihood, with slightly different parameters and, thus, some contentious standards issues to work out). But such third parties do not come cheap, and some may not deal well with third-world exigencies, such as physical danger and hardship (especially if the insurgency is ongoing), corruption, and incompetence. Finally, the public may well have habituated itself to a high level of state-security intrusiveness, thereby giving the host government more political scope to acquire police-state habits.

The ultimate safeguard against abuse of information capabilities is, of course, accountable local government—a fundamental goal of counterinsurgency. The United States is currently especially weak in developing justice systems—adequate courts, capable and honest judges, predictable and fair prosecution and appeals processes, and

humane and efficient penal systems—in countries facing real or potential insurgency. Strong independent justice systems are essential if the power of the digital age is to be used consistently in the public service. We would not advise the creation of the information-collection capabilities described in this volume unless accompanied by equally vigorous efforts to create such justice systems.

Conclusions and Implementation

Promoting the proliferation of cell phones while "owning" the switch can be a powerful tool for the U.S. government, and, by extension, the host government, to acquire information superiority in a contested area. Even if people are not altogether comfortable with the government tracking their cell phones, they do like their cell phones and may, therefore, be likely to put up with the first to have the second. As demonstrated, such a system can tilt the information world against insurgents and toward the government and its supporters, provide ready access by citizens to security services, and reap a harvest of information on where users are and with whom they are networking.

To engineer the cell phone system to support counterinsurgency, the U.S. government should support an implementation process with two steps: planning and implementation.

The planning phase, not surprisingly, will be relatively intense for the first such system designed to these specifications. It should likely be shorter, but not instantaneous, for all subsequent ones. The necessary tasks include

- establishing technical specifications for the switch and the handset
- engineering and coding the software for the switch and the handset
- developing and implementing a test and acceptance regime for the switch and handset

- developing the security features and designing a quality-control test for them (as noted, the more features, the more calls will be dropped, at least initially)
- in parallel, developing, coding, and optimizing algorithms and procedures for exploiting all the information that these phones are likely to produce
- designing contractual specifications for cell phone providers and test-marketing the phones to gauge their acceptability
- generating a registration protocol for domestic users and visitors.

Note that, for the most part, this planning produces a generic set of specifications and products that can fit almost any market equally well.

In the implementation phase, the actions are country specific. They include

- selecting one or more vendors (or coming to terms with existing vendors)
- helping/inducing the vendor(s) to build out the infrastructure (and possibly contributing some U.S. infrastructure, such as aerostats if ground conditions make it too hard to build or maintain cell towers)
- having an initial distribution of handsets manufactured
- registering users
- if there is an old system to be replaced, marketing the new system and switching people over from the old system.

CHAPTER FIVE

Embedded Video

Embedding video capabilities into military systems—notably, but not exclusively, small arms—has two attractive features: It provides material for lessons learned after engagements, and it creates a record of such incidents so that authorities can pursue or defend against charges of weapon misuse.

Linking the alleged use of force to video evidence is already common practice within U.S. police departments. 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.[1] Police officers, continuously aware that they were being recorded, learned to be on acceptable behavior at all times before the camera. More so, cameras became widely appreciated. No longer could errant citizens falsely claim that they had been abused by the police—as long as such purported abuse supposedly took place in the camera's line of sight.

In the conduct of counterinsurgency, interactions between soldiers and citizens can be equally problematic. In some ways, these interactions are more sensitive than they are for police. Misbehavior by a few "strategic corporals" can color every citizen's perception of all forces, notably foreign forces, and particularly U.S. forces. The citizenry may easily conclude that U.S. soldiers can be dispensed with (whereas few

[1] See Jess Maghan, Gregory O'Reilly, and Phillip Chong Ho Shon, "Technology, Policing, and Implications of In-Car Videos," *Police Quarterly*, Vol. 5, No. 1 (March 2002), pp. 25–42.

believe that society can do without police). Conversely, the conditions of counterinsurgency—in which, before insurgents strike, they are usually indistinguishable from citizens—make it difficult for even the most disciplined soldiers to avoid unwarranted harm.

Should soldiers, therefore, be equipped with similar cameras? Before answering "yes" wholeheartedly, it helps to examine some salient differences between police and soldiers to understand how such a system would work, the issues it may raise, and the role such cameras may play in warfare:

- Dismounted soldiers do a large percentage of their work far from their vehicles (and even when at or near them, the action is not always toward the vehicles' front—that is why, for instance, Humvee-mounted guns swivel).
- Soldiers in war zones tend to discharge their firearms far more often than do police, even those police with tough beats.
- Insurgents within one group are likely to operate in the same way, but every insurgent group is different in its doctrine. Criminals are likely to operate in different ways but one town's criminals are likely to be similar to another town's criminals. That being so, a systematic lessons-learned effort is likely to more fruitful in countering insurgents (because those encountered today are likely to act like those encountered in the past) than in countering criminals (where yesterday's criminals are not much like those of the present, but a general knowledge of criminal habits is expected of every police officer).
- Soldiers work in a heavy propaganda environment. Insurgents are more than willing to highlight examples of misdeeds by soldiers for political ends. Criminals have fewer potential sympathizers and much less money to publicize their stories.

Hence, the requirements for and the uses of such cameras will differ greatly.

Basic Concept and Technical Issues

The soldiers' equivalent of a dashboard video camera could be a device coupled to the scopes[2] found on most rifles these days—or, as some special operations forces do, mounted on their helmets. Similar cameras could be mounted on crew-served weapons, such as vehicle-based machine guns.[3] It would be nice if commercial-grade cameras would work, but testing will be required to determine what arrangements (e.g., hardening versus shock mounting) have to be made to ensure continuous availability in the conditions of combat—e.g., high temperatures, dust, smoke, and shock. Meeting the latter requirements may be expensive. Thus, such cameras may have to be initially reserved for soldiers operating "outside the wire" in insurgencies (a population of no more than 30,000 combined in Iraq and Afghanistan) plus sufficient extras for training, maintenance, and repair.

These cameras would operate continuously, recording everything[4] and bookmarking critical events such as a weapon discharge.[5] Soldiers

---

[2] This arrangement may create the temptation to photograph people by pointing a rifle at them (giving new meaning to the phrase, "to shoot a picture"). In the interest of avoiding the need to do so, some method for detaching the camera easily may be required, so long as it does not lead to such cameras being lost.

[3] For obvious reasons, it would be pointless to mount such cameras on weapons whose effects are distant or outside the line of sight, such as artillery, rockets, or bombs. The issue of whether to put GPS recorders on such weapons should be addressed elsewhere.

[4] There are two alternatives to continuous mode: event-loop mode and event-start mode. In event-loop mode, the video camera would write over material taken x minutes ago; if an event (e.g., weapon discharge) took place, material starting n minutes prior to the event and ending m minutes after the event would be subsequently locked from erasure. As the main text indicates, however, memory is cheap; battery power is what is expensive—and the camera would have to run all the time anyhow. Thus, the event-loop mode has no particular advantages. In event-start mode, recording would commence with the event (e.g., weapon discharge). This mode saves battery power, but it also provides no video information on what led up to the event. A compromise would be to take still pictures periodically, but the battery savings would be modest and the gain in information might also be modest. For these reasons, our discussion is limited to the continuous mode.

[5] Other types of events leading to a bookmarking, such as loud sounds or the appearance of a face in front of the gun, are possible. The fancier the processing needed to determine a bookmark, though, the greater energy drain.

would go on patrol or station with power supplies fully loaded and portable storage empty. When they return, 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[6] or by scanning forward to bookmarked events. The interesting material would be transferred to permanent storage (e.g., disk) as required. As circumstances permit (or, in the case of a controversial event, require), the disks would be collected and sent to a central location for archiving.

Among the potential constraints, memory[7] and long-term storage[8] are easy to deal with, but battery power[9] adds weight to weaponry.

---

[6] If taping is on intermittent loop, a soldier who has not discharged a weapon over the course of a mission will be coming back with only the last *x* minutes of patrol recorded.

[7] The amount of memory required for continuous recording is directly proportional to the resolution of the video camera, the degree of video compression used, and how long soldiers are out on patrol (assuming that they get new media upon return). To stick with commercial offerings as a basis of comparison, the choices are between a CD-ROM (700 megabytes) every two hours (essentially 320 x 240, VCR-type resolution), a DVD-ROM (4.5 gigabytes) every two hours (television-quality resolution), or an HDTV-ROM (in one incarnation, a 50-gigabyte Blu-Ray) every two hours (HDTV-quality resolution). Using the Apple iPod as a point of comparison, the storage can be either rotating (the 60 gigabytes of a top-of-the-line iPod Mini) or solid-state (the 8 gigabytes of a top-of-the-line iPod Nano). The memory devices in both iPods are relatively light, at least in comparison to the weight of a gun. Unfortunately, rotating memory tends to be shock sensitive. Overall, however, portable memory—which continues to improve rapidly every year—appears adequate for continuous-video capture.

[8] If we assume DVD-quality recording and 12-hour patrols, each soldier on patrol will be laying down enough video for a HDTV-ROM (Blu-Ray disk) every other day. At 300 patrol days a year for the aforementioned 30,000 soldiers, this equals 4.5 million disks or roughly 60 metric tons (or 180 tons if each disk comes in its own jewel case)—somewhat less than an M-1 tank. If only the material deemed interesting (e.g., the minutes before and after an event) is stored, far fewer disks are needed.

[9] A typical VCR battery, the Sony NPF-950, is advertised to run 15 hours and weigh 300 grams (10 1/2 ounces). As a general rule, weight and run time can be proportionately reduced. Unfortunately, until fuel-cell batteries become practical, little year-to-year improvement in specifications can be expected.

Evasion Techniques

The effect of everyone's actions being on camera all the time on the psychology of war fighting is not trivial. As a general rule, police cameras are purposefully turned on when police leave the vehicle. There is no real equivalent in war fighting. Unless there are strict protocols on what part of the recording can be viewed by others, there is an inevitable tradeoff between morale ("I'm not on camera all the time") and discipline ("I'm on camera all the time").

That soldiers may wish to exclude unfavorable events from being recorded is a real possibility. There are basically two ways to do so: Point the camera elsewhere at the time or eliminate the evidence after the fact.

One way to inhibit the former is to link the camera and the rifle scope, making it hard to disable the camera without disabling the rifle scope, but this is hardly foolproof.[10] There will be the inevitable work-arounds to permit the rifle scope to work without the camera, so the challenge is to make these work-arounds difficult to carry out or at least difficult to carry out without being obvious. Furthermore, soldiers intent on serious misbehavior may consider the lack of a rifle scope quite secondary. Conversely, a high percentage of unfavorable actions take place in the heat of confrontation and battle and, thus, without any prior thought of disabling the camera.

As for the latter, there are many ways to eliminate evidence, ranging from failure (of the camera, of lighting, of the memory device, of the process that delivered the memory from the gun to the command) to sophisticated ways of substituting benign imagery for telltale imagery. If media removal and rewriting seem to be a problem, the memory can be engineered so that it cannot be removed without breaking its ability to record further. But this solution will require specialized hardware (thus removing it from commercial economics). Also, at the cost of additional circuitry and energy, imagery can be digitally signed with

[10] Or risk free—if not done correctly, the normal run of problems with cameras may lead to scopes that cannot be used in the interim.

a tamperproof time source; if done right, this solution prevents rogue video from being spliced into real-time video.

Of course, it is up to command to inculcate each person's responsibility for the video, to ensure that equipment is working properly when soldiers go on a mission, and to set appropriate levels of suspicion when something appears to go wrong.

Technically speaking, however, the bottom line is simple: Embedded video is doable. The biggest problem is the additional weight that the battery will add to the rifle.

As a practical matter, the material collected will be too large to be on continuously spinning media (at least with today's, and foreseeable, storage parameters); however, some index to the material could be stored online. Thus, aside from material that has been edited and specifically posted for widespread review (whether by authorities or by individuals involved), access to video would be by request. If the total information content is measured in millions of gigabytes, then even using a disk jukebox for automatic retrieval will be infeasible. At any rate, making sure that no archive could be accessed without explicit permission by someone makes it easier to enforce privacy and security rules.

Uses

The primary purposes of these gun-mounted video cameras are to keep behavior among soldiers at high standards, so that they take action when warranted, or to exonerate and defend soldiers from erroneous accusations.

An important secondary purpose is as a learning tool, 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: for

example, a Wiki with connections like those of YouTube.[11] The value of video is that it helps avoid the work of reducing everything to written form—but the dependence on soldiers' willingness to learn based on their experience remains. If the material is to be used for after-the-fact review, then ground forces may end up adopting procedures already in wide use in the U.S. Air Force. Voice annotation or "chalk boarding" on the video itself may also enhance its value.

An occasional, but valuable, tertiary benefit is that the cameras may, from time to time, videotape people of interest. Indeed, gun-mounted video is far more likely to capture the face of someone shooting at a soldier than a random street camera is, and, being mobile and in the hands of someone prepared to shoot back, the camera is much harder to disable than a random lamppost camera. Video will make it easier to identify the person for subsequent apprehension.

If indigenous forces also adopt gun-mounted cameras, they, too, would benefit from similar learning opportunities and acquiring similar disciplines. This video would help immeasurably in on-the-job training, because their performance could be reviewed by U.S. instructors who could use them to offer tips and warnings.

Guidelines

Perhaps needless to add, if indigenous forces adopt such a system, they have to be suitably equipped, not only with compatible small arms, but also a sufficient electrical, electronic, and computer infrastructure (to recharge batteries as well as to download and convert video files). If the system is to be judicially credible, indigenous forces would have to exhibit the same discipline about collecting and maintaining records expected from U.S. forces. They would also have to be willing to share the records appropriately.

Also, privacy safeguards will be needed, perhaps like those governing police systems and other quasi-public monitors. Such safeguards

[11] YouTube is a popular Web video-sharing site that lets anyone store short videos for private or public viewing.

will need to set terms for when and for what reason the video files are reviewed and terms for who will have access to them. If the system is to be acceptable to those who carry rifles, whether U.S., coalition, or indigenous soldiers, there will have to be some reconciliation between such values and the generally intrusive monitoring that currently characterizes life in the respective militaries. In the civilian world, unions and their ability to call strikes provide countervailing pressure against the abuse of the system by managers. Unions have lead to the development of acceptable procedures for limited introduction of monitoring systems. Perhaps in the army, the long-standing tradition of reliance on noncommissioned officers for decentralized execution of higher command guidance may help guard against the misuse of monitoring systems.

It is important to think carefully about how to use the material in the right and wrong ways—which could easily kill the concept. The system is best *not* used for "Big Brother" type operations or for watching for the small stuff (except in informal unit evaluation). The system needs to be saved for what is important, and criteria for evaluating the latter needs to be articulated and justified before the equipment is used for that purpose.

Video Made Public

It is obvious that the public will be aware that U.S. (and perhaps indigenous) soldiers are carrying cameras.

With the realization that such footage exists, the local population will probably assume that such footage exists everywhere. The population will also assume that the failure to reveal such footage is some sign of guilt—even if such revelation would compromise operational security. If nothing else, U.S. and host-nation information campaigns have to anticipate that the population may reach such conclusions. Video is already popular in places such as Iraq; insurgents shoot a great deal of footage themselves and are not shy about distributing it over the Web.

The release of gun-mounted camera video into the public domain (especially in digital form) can be a large boon to the U.S. information

campaign if done promptly and intelligently. After all, there will be a large stock from which to choose, and if there is a story to tell with it, amalgamating the material should not prove difficult.

Insurgents will also be able to grab some of the same material, which should be taken into account. Normally, one risk of releasing digital video is that people can manipulate it to create false imagery (e.g., false or, more precisely, doctored still-camera imagery has surfaced in Lebanon). Fortunately, if the frames are digitally signed (see above), manipulating the video or inserting false frames into it will be immediately detectable. The bad news is that the technique by which the material can be determined to be false is hard enough to explain to Western audiences who are technically sophisticated and apt to trust technical experts. We can only imagine how much harder such an argument would be to make elsewhere.

Conclusions

Embedded video is simultaneously an accountability device and a lessons-learned device (when cameras are detached, they can also be used for recording observations). More broadly, embedded video is an information device, recording events as they take place and using the awareness of such recording to improve performance.

To make this system happen, the U.S. government will need to carry out what we believe to be a modest program of research, development, and acquisition to procure weapons with associated cameras (vehicle-mounted or free-standing cameras present fewer technical and procurement challenges). Once acquired these would be issued to front-long operators directly (if in the U.S. military) or indirectly (e.g., on discretionary terms for indigenous operators). The follow-on step is to institutionalize the process of collecting the data, scanning them for interesting material, and ultimately moving the peta-bytes from the field to their ultimate repositories.

CHAPTER SIX

A National Wiki

Knowledge about the indigenous community is a critical requirement for both long-term stabilization and episodic operations. Indeed, almost 20 percent of the 160 data items in the Appendix require knowledge of the social, political, and economic structure where operations will be taking place.

The normal way for militaries to get such knowledge is to send out intelligence operatives to look around and ask questions. Even in today's information-rich environment, there is no substitute for this activity, but its efficiency remains little higher today than in biblical times—and such operators are "thin on the ground." Even in Iraq, intelligence officers number only in the hundreds. If potential information sources are expanded to include U.S. operators who spend serious time "outside the wire," the count is less than 30,000. This number pales in relation to the population of all military forces, notably indigenous ones. Military forces, in turn, are a fraction of all government employees in the country. All these are dwarfed by the size of the overall adult population. Furthermore, U.S. intelligence officers are rarely as steeped in the local culture as the natives are (although the truism that fish do not see water is apposite here).

On the theory that numbers count, especially for coverage, why not recruit the local population to reveal the ways and means of their respective communities? Hitherto, this commonsensical notion has been overlooked, largely because of some practical difficulties. In the absence of functioning mail or phone service, not to mention widespread adult illiteracy, the only effective means of communications was

face-to-face conversation, but the residents speak a language that cannot be understood by most U.S. soldiers. Even if a common language is used, soldiers too often lack the context to know whether or why what they hear is meaningful or to prompt people for further information. If information is passed orally, soldiers must be relied upon to retain a sufficient percentage of what they heard—and with enough detail, accuracy, and background to be usable. Whatever information *does* finally work its way into records (assuming there is a decent record-keeping system for such material) should be amalgamated, categorized, sorted, and made readable for use. To be sure, word-of-mouth intelligence has often informed warfare, but it requires a large number of motivated people, not least of whom have to be the locals themselves, to gather some information at all. If there are no prior contacts in an area, there is also no word of mouth—and, thus, nothing to prepare people coming into an area for the first time.

In today's information age, there has to be a better way to generate and share all this local knowledge.

In fact, there very well may be such a way, and Wikipedia may be one such model. Wikipedia is a specific instantiation of a Wiki, a Web-based method of amalgamating knowledge on a subject.[1] A Wiki

---

[1] Wikis, blogs, forums, post-its, chat rooms, and instant messages, while related, differ. A blog is someone's journal, which can be about practically anything, from the deeply personal to intensely topic focused. As such, they are more likely to be discursive and opinionated. Blogs are generally sorted from the latest post to the oldest post in a series (with yet older posts available in archives). Writers can edit their previous posts (and the edits are often obvious). Some blogs permit user feedback, which is also posted.

A forum (or chat room) is similar to a blog in that it has an initial entry followed by user feedback. Postings to chat rooms are generally organized by topic (not author) and sorted, within each topic, by the date of entry. They often have editors, who need not be (and, usually, are not) the same person who wrote the lead-in entry. These editors can censor material or redirect entries to a more appropriate subject category. In a lively forum, there may be several subthreads of discussion running at the same time, and, thus, it is not always clear which prior entry a comment is addressing. Kind posters often repeat the entry within the text of their message before commenting on it.

A post-it would be a comment with an obvious visual link to what is being commented upon (so that an entry would be linked to its comments as well as a comment to that which it is responding). Post-its, as such, have yet to be implemented, but a feature in Google Earth that allows readers to annotate comments to particular points on a map comes close.

is a posted narrative that others can edit for accuracy, tone, or whatever strikes their fancy. Edits overwrite previous material. Readers do not see the equivalent of tracked changes (as in Microsoft Word), but an explicit history of changes is kept for the benefit of those who really need such information.

A core 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.

In describing a national Wiki, assume for the nonce a computer-owning population that writes in English. Granting that such a circumstance is highly unlikely in today's or even tomorrow's insurgencies, it is a conceptual placeholder for the discussion on how to build such a system over cell phones and what to do about translation into English.

Our Town

A national Wiki, so to speak, would be a compendium of information on the country, organized by topic, but with a large chunk of it geospatially linked and, thus, in theory linked to points on a map[2] (as Google Earth can do).

A chat room is similar to a forum except that the material is more evanescent and entry to a chat room is often limited to specific individuals (in many cases, a user must be invited by someone already in the chat room).

Instant messaging is similar to a chat room except that it is more convenient to use and is often more akin to a two-person telephone conversation.

[2] For example, users of a national Wiki could be given a country map from which they could zoom and pan to the region of interest. Icons on the map would be linked to material on specific places. Moving a cursor over the icon and clicking it would bring up a menu of the material from which a selection can be made.

Submissions to a national Wiki could range from a full-length treatment of a topic to a minor comment. Unlike Wikipedia[3] itself, the material need not be definitive. Nor need everything on a topic be an edit to preexisting material. We might consider that topics are less like encyclopedia entries and more like starting points for a discussion. A strict encyclopedic format might be off-putting or at least strange to a population whose members had likely never seen an encyclopedia and fewer of whom were capable of writing a coherent and well-organized encyclopedia article anyway. In contrast to Wikipedia, a coherent national Wiki may require more than a modicum of external editing—but this should be an acceptable price to pay to maximize inclusion.

Why would people want to contribute their observations anyway? Pride would likely be the primary motivation. First, if a national Wiki is well-known and sufficiently accessed throughout the country, each contributor would be able to point out the contribution that he or she made (even if not identified as such). Second, people feel pride in their hometown or neighborhood, and many need little prompting to describe its features to strangers, even if these strangers are U.S. forces—perhaps especially if they are U.S. forces.

Initial contributions are apt to prompt further contributions.[4] The more people contribute to a national Wiki, the more that other people will read it, which means that further contributions are likely. Others

---

[3] Wikipedia is a particular Wiki, and it comes with its own rules and conventions. First, the material presented is of encyclopedic form: that is, each entry is limited to a single topic (and each topic appears only once), is definitive (rather than ruminative) in its scope, and is presented with a neutral point of view. Second, the use of a word in a text is highlighted if the word, itself, is another topic heading; clicking on the word will bring up the article associated with that word. Third, both the contributor and the editors are, if not anonymous (this has varied over time), not revealed to the reader. Fourth, editors can exclude specific users or prevent entries from being modified; the German version of Wikipedia started experimenting with the requirement that all input pass through editors before being posted (Bill Thompson, "Not as Wiki as It Used to Be," *BBC News* (August 25, 2006). As of June 11, 2007: http://news.bbc.co.uk/go/em/fr/-/2/hi/technology/5286458.stm.

[4] Significant contributions could also be rewarded explicitly, with, for instance, phone cards—which is easy to do, especially if a phone company hosts the national Wiki. Accepting such a reward may well identify the author.

will be impelled to contribute to amplify a point ("he mentioned Mr. X but ignored the contribution of Ms. Y") or refute one ("he said it's white, but it's really beige") if such points vie to be the quasi-official truth. Again, judicious editing will be required to preserve as many contributions as possible while avoiding the flame wars that are common in cyberspace.

Many contributions will be opinionated, and that is both tolerable and enlightening. Indeed, if the contributors to a national Wiki are sufficiently representative of the population (or at least that part of the population that should be heard), it can be a useful place from which to gather information on what the population thinks about the parties to the insurgency.

Similarly, if a national Wiki is sufficiently popular, merchants and others (perhaps clerics) will see it as a vehicle for advertising (or proselytizing). Although a little advertising is not entirely bad (and may also provide useful insights for U.S. forces), too much of it can reduce readership. A tawdry reputation can also inhibit those who have something serious to say from making their contributions.

Pride (or even greed), however, may not be enough to prompt contributions, particularly in the beginning when material is scant and readership is relatively light. Kick-starting this project may require funding people to write initial articles. The outlays are unlikely to be expensive (given prevailing wages in countries prone to insurgencies). Besides generating articles, the effect of funding would be to draw in the country's underemployed intelligentsia, people who are apt to be the more critical opinion makers.[5] It is often amazing what kind of allegiance money can buy, especially if the transaction is reciprocal (as it would be in this case), rather than make-work or, worse, a bribe. Later on, funding can be used to spread out the coverage, acting as a counterweight to the natural tendency of people to focus on popular hobbyhorses to the exclusion of more serious topics (which is to say,

[5] Compare this, for instance, with the Federal Writers' Project of the Depression-era Works Project Administration.

topics helpful to counterinsurgency).[6] Less tangible and more symbolic awards, bragging rights and generally favorable publicity, can also help motivate contributors.

Apart from editing, some work will be needed to find or develop a useful superstructure for the contributions so that they can be found not only by U.S. forces, but also by potential contributors and the mass of users. As noted, maps are one example; there may be others (in many countries, for instance, there is a great deal of familiarity with how religious texts are organized).

It cannot be overstated how important it is that this Wiki be seen as a national, even nationalistic, enterprise, and not one used to feed intelligence to U.S. or even host-government forces. Part of supporting this perception is acting as if it were true and treating the Wiki as yet one more open source monitored by the U.S. government. Thus, ensuring that editing is transparent if not minimal and that it is unbiased in that it does not filter out anti-American opinion are important.[7] Laundering the money for contributors through the host-nation government or a third-party organization may also be recommended to limit traces of U.S. influence (but between rumors and the belief that anything that aids the United States must, therefore, have been U.S.-created, this may be an uphill battle).

What prevents the insurgents from exploiting the information in this Wiki? Nothing. But U.S. forces are likely to have less local knowledge and context than local insurgents do; the same holds, to a lesser extent, for the indigenous army (indigenous police would more likely know their way around). Therefore, anything that makes the coun-

---

6 In Wikipedia, computer games, for instance, rarely lack for long and loving articles. Or, as comedian Stephen Colbert observed, the entry on "truthiness," a word he invented, is longer than the one on Lutherans. He may as well have added that his biographical entry is longer than that of Jean Baptiste Colbert, the French finance minister who invented mercantilism and without whom Louis XIV, the Sun King, would have been just an everyday monarch.

7 An open question is whether to make certain topics off-limits as irrelevant. It is not inconceivable that in many Arab countries, there will be a great demand to opine on Israel. The cost of blocking such material may be substantial in terms of local support and even credibility. The benefits of censorship are harder to discern.

try more understandable to anyone works to the net U.S. benefit. If a large percentage of the insurgents are from outside the country, then they might learn something, and so the net gain would be lower, but, even so, most outsiders who come for the insurgency are likely to have more cultural knowledge than U.S. forces will. An important secondary benefit should not be overlooked: If a national Wiki is embraced as a host-government project, then the government gets credit for whatever the citizenry finds positive about it.

An Oral Wiki

It would probably be worthwhile for the United States to encourage the connectivity of countries' citizens, especially those under the threat of insurgency. Familiarity with information systems promotes literacy and numeracy, and it stands a country well in international economic competition. A literate population, in turn, is one likely, for that reason, to favor democracy and hold governments accountable. Nevertheless, because many countries prone to insurgencies are too poor to benefit from widespread computer ownership, some thought may have to be given to alternative ways of accessing a national Wiki. A literate population that surfs the Web through public channels—e.g., cybercafés or kiosks—while less implausible, is still unlikely. But it is not hard to imagine that most adults own cell phones, especially, if as advocated earlier, such services were encouraged. Where there are cell phones, there is potential Internet service, from simple messaging to more complex small-screen Web surfing.

Can the Wiki experience be duplicated over a cell phone? Perhaps, but it would be challenging and may require some research and development to make happen.

Two models can be envisioned. One model assumes that those most willing and able to submit material will be literate and motivated

to seek out available computers for the task.[8] If, however, the literate elite in a country writes in a language that differs from that of the rest of the population (or a large fraction of the population), translation will be required to make the articles broadly accessible. Users, in turn, will come in two types. U.S. operators and the wired locals will access the material via computers; the rest would acquire it on their cell phones.

Although this adaptation comes closest to the Wikipedia model, it may not work well. If a mass audience is desired for such a Wiki as a way of encouraging contributions, both directly (by the masses) and indirectly (because contributors get mass readership), then the small screens of cell phones may be unsatisfactory.[9] Cell phone screens are simply not well adapted to reading, particularly anything very long (MP3 players and game machines make do with individual words and small phrases). They are even less suited for writing, as attested to by the short length of messages sent by users of Blackberries (which, unlike most cell phones, come with full keyboards)

The second model relies almost exclusively on oral input. Those limited to a cell phone can still declaim about this or that feature of a city or neighborhood by talking about it. Indeed, if cell phones are equipped with cameras (as most are these days), it is easier to make a walking video commentary of a city or neighborhood with a cell phone than with a camera plus a computer.[10] The effort might as well be subsidized by making the creation, transmission, and reception of Wiki

---

[8] Finding word processing software in languages such as Arabic and Spanish may not be difficult, but it will take money to ensure the existence of word processing programs for less popular third-world languages.

[9] The cell-phone-cum-iPod that Steven Jobs introduced at MacWorld (see Ryan Block, "Live from Macworld 2007: Steve Jobs Keynote," *Engadget,* posted January 9, 2007: http://www.engadget.com/2007/01/09/live-from-macworld-2007-steve-jobs-keynote/) sports a fully functional browser, suggesting that such devices are getting closer to the point where reading is feasible on them. The market will determine whether such devices are actually used that way.

[10] Cell phones that record the global position of the caller can be programmed to do so frequently for national Wiki submissions, thus making it clear what area is being referred to as the submitters walk.

materials free—something that follows easily from "owning" the cell phone switch.

Unfortunately converting a Wiki into an oral format is anything but easy. One problem is sound quality, especially if the material is recorded on the street (as might be appropriate for street-level commentary). Automatic cleanup is not impossible, but the results may be less than perfect. A voice recording is good for short annotations, but anyone who has ever tried to leave a long phone message knows its inadequacies. They persist even if someone takes multiple chances to redo the message or is allowed to build up the message one short block at a time. A more serious problem is editing someone else's submission. Breaking into a written narrative to insert words is easy; breaking into a voice narrative to do so is tricky and the results, if successful, would sound quite strange. Editing would probably have to be done via annotation ("he said the building is red, but it is really yellow"). Such annotations would require the listener to hear out all the comments (and decide which comment referred to which item) or to an editor to use an organizational scheme to get it to make sense. The latter, although somewhat artificial, may be better.

Another issue is how to help users find and listen to what has been submitted. Material associated with a specific place might conceivably be located by giving users access to a virtual map of the country and allowing then to pan and zoom as needed to the appropriate link. But this leaves out many worthwhile topics that do not map particularly well. To find them will require that contributors annotate their oral inputs with some sort of header (and, of course, some of them will already have been used, leading perhaps to a numbering sequence for the headings), which will require some sort of keyboarding prior to submitting the material. In a heavily edited process, there should also be a feedback mechanism so that users can see what happened to their submission. Users may have the choice between calling on such material via keyboarding or, perhaps more felicitously, through pull-down menus (as can be done to look up articles in the electronic version of *Encyclopaedia Britannica*).

Compared with a written counterpart, a national oral Wiki is likely to differ even more sharply from the written Wikipedia. Sub-

missions will require more "official" editing but will likely receive less unofficial editing from other contributors. In general, submissions will also be shorter. By design (and consistent with oral input), they are likely to be more poetic and less prosaic, as well as more discursive and opinionated. Searching by title will be the norm, but searching by content will be difficult if not impossible. On the other hand, such a Wiki is likely to have more multimedia content mixing commentary with pictures taken by camera phone.

The ultimate form of an oral Wiki is hard to predict. The essence and some choices are sketched here as a way of suggesting how it might work. Someday someone may want to build a similar capability somewhere in the world. If so, it is a near certainty that approaches to such problems undreamt of in this narrative will emerge—it remains for cell phone software to accommodate such approaches.

Attribution

Wikipedia articles are not signed; given the norms of cyberspace, there is no way even for the editors to know who really submitted what (although the president of Wikimedia Deutschland has a list of its thousands of authors). By contrast, contributors to the *Encyclopaedia Britannica Online* are visibly identified (if you know where to look).

Anonymity in submission has pros and cons. If people believe they are anonymous (which is somewhat correlated to their really being anonymous), they are apt to be more fearless in their reporting. This is no small matter if they are to tell the truth about the power structure or report something about someone who settles grudges violently, a habit not unknown to insurgents or counterinsurgents for that matter. But the same lack of ascription may also provide a cover for irresponsibility, leading to inaccurate or even slanderous submissions. True, the editing function of Wikipedia, for instance, limits the damage that might result, but not entirely: In May 2005, an anonymous user (later identified) created a five-sentence Wikipedia article about John Seigenthaler that associated him with the assassination of Robert Kennedy and that lingered largely unchanged for four months, until it was brought to

the subject's attention. Furthermore, as suggested, the with-so-many-eyes-all-inaccuracies-are-shallow rule that people have associated with Wikipedia may not necessarily apply to a national Wiki (which would have fewer eyes). Finally, submissions that come via cell phone may be easy to trace, especially if, as discussed above, the system has strong traceability.

Should contributors be acknowledged? The anonymity of Wikipedia follows from its being touted as a community effort, in which peer editing is central. A national Wiki for which peer editing is less central may usefully lean toward identification, with the permission of the contributor, as a way of inducing further contributions that someone can point to as his or her own.

Language Translation

As noted, there are two translation problems. Contributors may not write or speak in the language of the majority or even large parts of the population. More commonly, U.S. war fighters will not know the language in which the material, whether oral or written, is submitted. In either case, some provision should be made for translation.

Direct translation should not be a difficult problem. Paying for translation services is one way for the United States to spread the wealth to a grateful population (and, again, translators are likely to appear disproportionately among the intelligentsia). Nor should translation necessarily be expensive; the number of submissions is likely to be measured in myriads not millions.[11] Furthermore, not everything need be translated, because only a small percentage of a national Wiki is likely to be useful for U.S. operations—something native speakers can make a first cut at determining.

It bears repetition that a national Wiki would be a national project, albeit one supported initially by U.S. funds. The real version is in the foreign language. The translated version is just a mirror. Prob-

[11] The English-language version of Wikipedia had 1.6 million articles as of early March 2007.

lems in translation for outsiders cannot be seen as preventing the project from going forward and serving the nation as a whole, even if the benefits to counterinsurgency are the raison d'être of the whole project. Anyway, those who want to see everything in order to get a fully nuanced picture of the country would be better advised to learn the language in the first place.

Translators ought also to be alert to cultural context. References to this or that historical or literary figure, for instance, are often references to a particular narrative, myth, or moral. The association of a location with a religious figure of centuries past may communicate something important to locals while meaning nearly nothing to Americans. So these metaphors will need to be annotated in the English-language site.

Accuracy and Deception

How reliable will the material in such a national Wiki be? What prevents ill-wishers from submitting material that is deceiving? As already noted, if a topic is popular enough in Wikipedia, the chances that serious errors will remain uncommented upon is sufficiently low. A well-cited article in *Nature*, concluded, for instance, that Wikipedia's error rate was not much higher than that of *Encyclopaedia Britannica Online*.[12]

---

[12] Jim Giles, "Internet Encyclopedias Go Head to Head," *Nature*, Vol. 438 (December 15, 2005), pp. 900–901. Specifically, a comparison between *Encyclopaedia Britannica Online* (EB) and Wikipedia on the same selected science topics showed little difference in their accuracy. The average EB article had three errors and the average Wikipedia article had four. EB's management was outraged, and Wikipedia's was delighted by the report. EB issued a spirited rebuttal claiming that *Nature* had made methodological errors and that half of their so-called errors were either not errors or valid differences of opinion. Nature's editors were kind enough to post the details of their assessment, analysis of which suggested that the quality differences between EB and Wikipedia were understated by the article. Because Wikipedia's editors offered no rebuttal, it is unclear what percentage of errors found in Wikipedia were, in fact, errors; thus we cannot say what the true error ratio was. The more fundamental difference, though, was the presence of the more serious errors in Wikipedia, including several instances in which reviewers simply did not understand what some material in Wikipedia meant or referred to or why it was there.

Because similar mechanisms would be used in a national Wiki, similar self-correction mechanisms are available. It remains to be seen how much of a difference it makes that the list of contributors is likely to be smaller and that oral submission may be harder to edit than written submissions. Furthermore, accuracy issues are likely to be worse in cultures in which people are prone to substitute what they would like to believe is true for what is, in fact, true—and while no culture is immune, some are more heir to this tendency than others.

The problem with inaccuracy is twofold: its effect on the naïve user and its effect on war fighters. In both cases, we should look into the alternatives. Accuracy in the native media is not perfect, for instance. At least with a national Wiki, a self-correction mechanism allows for a check on accuracy that the self-interested media do not.

The effect of a deceptive error on war fighters, however, may be substantial, especially if it leads to their misreading the environment in which they will be working or fighting. To be sure, conventional intelligence inputs are, themselves, often wrong (e.g., sources self-servingly lie and analysts make mistakes), and because they are compartmented there is much less opportunity for any self-correction mechanism to kick in. It is much rarer, though, that the intelligence community deliberately deceives operators.

Here is where the fact that the material has to be translated may come in handy. In the translated version, the intelligence community can append commentary. Indeed, there is no reason why operators, themselves, cannot comment as well. While the authorship should be authenticated (verifying that the author is a U.S. operator), permitting contributors to stay anonymous may yield better results. Accuracy in reporting or commentary requires ignoring the natural tendency of a chain of command to censor reports from below that may contradict the official line.

Commentary from U.S. government representatives are likely to be sensitive, not least because negative comments will be seen as commentary on the veracity of the local population. It may also be perceived as a window into what the U.S. official knows and thereby implies something about sources and methods. At a minimum, there-

fore, such commentary should stay in the English-language version of the DoD Intranet and not via the publicly accessible Web.

A National Wiki as a Feedback Mechanism for Government Services

It is but a small jump from a national Wiki as a way for everyone (including U.S. forces) to learn about a nation's communities to a national Wiki as a way for the people to talk to others in the population and, not incidentally, their government.

Several years ago, New York City established a "311" service that could be called by anyone needing a city service whether or not they knew which of New York's over one hundred agencies dealt with the issue at hand. The caller does not have to navigate the city's bureaucratic maze to get service. Part of this was accomplished by having city-wise phone operators, which is necessary if the problem requires nontrivial dialogue.

Can a national Wiki be used as a mechanism for a similar service in insurgent countries? On the one hand, the service would have to cut across all layers of government to the extent that citizens are unclear about what part of government has which duties. On the other hand, the complexity of governance is likely to be far less than that in New York City (well over a hundred agencies are listed at the www.nyc.gov Web site). Even in nations that have little cross-government expertise, some headway can still be made by logging the complaint and either inferring the rest of the information from the situation ("oh, that's why this pothole should be fixed now"). Assuming the use of the cell phone system of Chapter Four, a callback number could be easily associated with the complaint; because of the system's GPS capabilities, references to "here" could also be interpreted more or less accurately.

Of note, particularly for insurgent-prone countries, such a scheme would put the onus on the government to find and fix the problem—and not on the caller to petition the government. What would give this service a Wiki-like character would be the government's responsibility to state what was done in response. The government could be

lying, but the complainer (or a neighbor) could respond as much. All this could be public knowledge should the caller so wish,[13] and having the complaint, the response, and the overall feedback trail accessible would reveal how responsive the government actually was.[14] Not only would the interested public know, but so would U.S. authorities, both locally (e.g., the lieutenant colonel leading the detachment in town) and nationally. As noted repeatedly here, one key to government legitimacy is good governance, and while scorecards alone do not automatically raise the score, it is hard to imagine doing so without them.

U.S. forces are also likely to be the butt of some complaints—and this is as it should be, even if the capacity to complain risks becoming a lightning rod for the occasional anti-American dog pile. Think of it as a service provided for U.S. forces by the citizens in an effort to keep such forces accountable. To be sure, many of these complaints will be groundless, and a fair percentage of them may well be posted by the insurgents themselves. But this is where the gun-mounted cameras come in handy. If the complaint has even a smidgen of basis, there should be some video that can address the incident in ways analogous to how dashboard cameras (usually) vindicate police so accused. The more that such complaints become the focus of local attention, the more aware the citizenry will be that U.S. forces carry video cameras with them as part of their weaponry. If indigenous forces are so equipped (as they should be) the same credibility could carry over to them as well.

---

[13] Many complaints to the government—e.g., get my cousin out of jail or help me with this health problem—may not be of the sort that callers want known to the world.

[14] Needless to add, this is a sketch of a service with many implementation details to resolve. That part of a national Wiki will need neutral editing to eliminate undesirable material—such as crank calls, spam, or personal slander—as well as to eliminate errors (e.g., mismatches between complaints and responses). The back-and-forth trail has to be readily accessible—which means it has to be indexed in some logical manner. The editors, for their part, have to be on someone's public payroll, but not in ways that would lead to charges that they were censoring rather than simply cleaning up the dialogue.

Conclusions

The establishment of a national Wiki would be a modest but significant step in understanding the human terrain over which insurgencies are fought. A national Wiki would elicit information otherwise unavailable through other methods. Allowing anyone to comment on the information provides a check on the tendency of such materials to vary from the truth. A national Wiki, once established, can also serve other uses, not least of which is to create a vehicle by which citizens can talk to their government—with the government's response available for all to see.

Simply establishing a national Wiki on the Web is easy; they already exist in a variety of languages. Thus, the effort would require little more than buying or leasing server space, getting a domain name, and publicizing the effort. However, a Wiki of sufficient detail to be useful may require other inducements. Hosting the Wiki over a cell phone system, while possible, would require working out several design issues and may require research and development.

CHAPTER SEVEN

The Principles of ICON

Prior chapters have proposed several ideas for generating information: the registry-census, the national CAD model, an expansion of the cell phone infrastructure with reliable links between the phone and its owner, embedded video cameras, and a national Wiki. Because naked information is of limited use, we have to then ask how best to make the material available to users. Specifically, what kind of information system should the United States employ to conduct counterinsurgency most effectively? How can the system best serve users (rather than some externally determined set of users' needs)? How best can timeliness, reliability, and security be balanced? How can we integrate in one system the information supplied by the intelligence communities, the "proceeds" from street-level operators, and the information that only the population can provide? How can such information capture the complex dimensions of the human terrain over which insurgencies are fought?

At heart, many of these questions are people issues, for two reasons.

First, because the key aspects of ICON, as will be shown below, are about 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 on. Because the relationship between U.S. and indigenous forces in a counterinsurgency matters more than that for conventional warfare, determining who can see what information is all the more critical. Deciding on such policies (as commanders should) necessarily precedes enforcing the policies and also precedes

deciding what kind of network is required to enforce such policies (a matter of engineering and systems integration).

Second, because as argued in Chapter One and explained more fully in a companion volume,[1] it takes a great deal of distributed cognition to counter insurgency well. In systems terms, the interfaces between counterinsurgents, insurgents, and the population is broad and highly variegated. Every insurgency is different, and even single insurgencies can be composed of many loosely coupled pieces. The problems of counterinsurgency are 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. It is only a small exaggeration to posit that every counterinsurgent must figure out the war on his or her own. Cognition, of course, matters for conventional warfare as well, but a far larger percentage of the problems of conventional warfare (as the United States fights it) involves how to make defense systems and organizations do what they are supposed to do. Such problems can be hierarchically decomposed into successively smaller and finely detailed chunks. Thus, *the information required to solve such problems can be compartmented*. When systems integration is required, it can be concentrated among defense contractors (for defense systems) or commanders and their immediate staff (for organizations); and they, in turn, enjoy broader access to information. Conversely, because the problems of counterinsurgency cannot be so easily decomposed, compartmentation of information gets in the way of resolving these problems. Counterinsurgency operators need both the information support and the cognitive capabilities to deal with a set of much broader problems.

This emphasis on the thinking user forms the case for ICON's most important principle, user primacy (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

---

[1] Gompert, *Heads We Win—The Cognitive Side of Counterinsurgency (COIN): RAND Counterinsurgency Study—Paper 1.*

of insurgency, both follow from the argument that, sooner or later, and preferably sooner, an insurgency has to be won by indigenous forces. In light of the time-tested principle that insurgencies are battles over legitimacy and governments, these forces include not only indigenous war fighters but also police, political leadership, and civil servants. These principles together require a shift away from compartmentation (essentially information denial) as the primary tool of information security. We suggest, therefore, that ICON rely, instead, on robust auditing, the third principle.

The remainder of this chapter discusses, in turn, each of these seven principles:

- Emphasize user primacy, inclusiveness, and integration.
- Build ICON to go native.
- Audit, audit, audit.
- Tune ICON to the level of insurgency.
- Post before process.
- Establish a standard deck and populate it from a national Wiki.
- Rank information by reliability and relevance.

Principle 1: Emphasize User Primacy, Inclusiveness, and Integration

By user primacy, we mean that 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; integration because internal boundaries frustrate collaboration.

The value of user primacy, inclusiveness, and integration are well demonstrated by the Internet. Users can communicate and thus collaborate with virtually whomever they wish. Search programs ensure that users not only get the information they need but also influence what information is posted. Web sites and Web logs let users inform

other users. Wikis collect and share information by topic. With each passing year, the likelihood that some relevant information on a topic is posted somewhere rises toward certainty. To be sure, the Internet has shortcomings, especially its insecurity; but its billion users accept this as a price worth paying for an open-knowledge environment that helps them function and learn. Because Internet protocols come standard, heterogeneous computer environments are far less of an obstacle to integration. So, the technological foundation for user primacy is well in place. Only political, bureaucratic, and security barriers remain to constrict user access and collaboration across agency, international, and foreign-local lines. In sum, user primacy, inclusiveness, and integration have prevailed in the larger information world because they offer enormous practical rewards to individuals, enterprises, and markets. Similar principles would permit the more effective exploitation of information in counterinsurgency and thus more effective counterinsurgency.

To the extent that traditional defense systems stress provider control over user primacy, security over access, and bureaucratic prerogative over timeliness in information distribution, they contravene such principles. All too often, non-Americans get access to U.S. information only by exception. U.S. security organizations, especially military and intelligence services, tend to limit access to information, to compartmentalize it; headquarters gets priority over those in the field. Similarly, networks and the data they carry are regarded as belonging to command hierarchies (e.g., regional joint Combatant Commands) and information providers such as the intelligence community. Those who need information have less influence than those who have it. Making information a strategic resource for counterinsurgency requires nearly the opposite of the way information networks are designed and managed for U.S. military and intelligence uses today. It will take a new philosophy—one that presumes that users have to think about, and not merely apply, information—to succeed.[2]

---

[2] Although this chapter argues that counterinsurgency needs an information system (i.e., ICON) that matches the breadth of the counterinsurgency problem, we have also noted that, if it is to work well, its users should also have a similar intellectual breadth, and we advocate as much in a companion piece. Yet, a large share of the users, ultimately growing to 100 percent of them, will be indigenous operators, and they too cannot exploit ICON without a

With the need for user primacy, inclusiveness, and integration in mind, we examine how the United States can make better use of information to prevail over today's insurgents who have proven themselves sophisticated at using information technology for their purposes.

ICON, in contrast to current military systems, would be designed around the principle of open access to information in two senses of the term. First, information would be available to every user as soon as it is available to any user; whatever analytic services are required to dress up the information would be provided à la carte, as it were. Second, information security would be provided not through a cascading series of restrictions, but also by a heavy emphasis on auditing what people do with the information (in contrast to what information people have). However, the various methods used to ensure the integrity and availability of ICON (e.g., protection against the insertion of malicious code) would be similar to those of any highly reliable computer system built on the premise that not all of its users are necessarily trustworthy.[3]

To illustrate how an alternative method of balancing security against other, often more important features, such as reliability and timeliness, consider the information system used by U.S. war fighters in Mosul (circa 2004) as an arrangement that points to some of ICON's features. There, intelligence operatives in Iraq were placed under the direct operational control of commanders rather than their parent agencies. The results at the time[4] were apparently favorable. The underlying principle that information sources be much more directly under a field commander's control has a great deal to recommend it. It helps focus the intelligence detachment on the needs of the war fighter rather than on the needs of the intelligence bureaucracy, short-

comparable intellectual breadth. How to foster such breadth among indigenous operators is a challenge, although not an insurmountable one. Addressing this problem was beyond the scope of this work.

[3] We, thus, differentiate between the governing policies that are designed to determine who gets access to what information and the administrative policies designed to ensure that the governing policies work as intended.

[4] Given the many ups and downs of that part of Iraq, our assessment is based on conditions prevalent at the time the system was used.

ening the time between when information is discovered and when it is shared—a tendency entirely consistent with the prior principle of making value-added services voluntary and letting users have access to the raw material sooner. The fact that field analysts are figuratively and literally further from headquarters, and thus further from national assets, may not be so harmful. Although national assets have no substitute for monitoring denied areas, in counterinsurgency, though, the United States would already have forces, allies, and equipment in theater. If imagery satellites can view something, then so can unmanned aerial vehicles. The signals intelligence that can be acquired by using assets under national control can also be acquired by in-theater devices, which, for this reason, are closer to the signal to be intercepted. The human intelligence sources managed from afar may be managed as well, and probably better, by local operatives; their proceeds can be complemented by local informants and tips from the population. If the cost of using national assets is that U.S. forces cannot share and thus coordinate with indigenous forces, this cost is too high. The tradeoff between what should be protected and what should be made available is almost always better decided in theater than across the globe. The clearly preferable choice is for an information system under the control of local commanders that lets them fight the insurgency as they deem fit. Do not be surprised if their take on intelligence is "if we can't share it, we don't want it."

The Mosul adaptation points toward but does not actually embrace the principles of ICON proposed here. The horizontal sharing of information, under the direction of operating commanders, did improve timeliness by relaxing vertical control of information. For the sake of getting information quickly to use against fleeting insurgents, the commanders were willing to forfeit whatever information security was afforded by vertical control. Presumably, they felt that escaping insurgents were worse than escaping information (that was most likely perishable). From an operational standpoint, this seems like a good trade.

However, what was attempted in Mosul did not improve the reliability of the information. Indeed, insofar as increasing the speed of shared information results in reduced screening, verification, and anal-

ysis, reliability could be reduced. Yet, as noted here, reliability is as important as timeliness. Unreliable information makes counterinsurgency more error prone. Errors in conducting counterinsurgency, particularly regarding deadly force and detention, may have severe consequences, not only for the scene of the error, but potentially worldwide. The question, then, is "can networking that improves timeliness retain or even improve reliability?" The answer turns on whether top-down control of information, which clearly causes delay, is essential for reliability as well as security. We have our doubts that it is essential, at least with regard to counterinsurgency.

Recall that most of the 160 information requirements identified in the appendix could be met—indeed, could best be met—by information from the population and other users, not from hierarchies (e.g., headquarters) or secret intelligence sources. The reliability of a report about nearby insurgent activity is more readily checked by communicating with people or other operators nearby than by referring it up a chain of command that may be, quite literally, clueless. Reliability is an information challenge in any case, and while it should not be sacrificed for the sake of speed, the principles of ICON should not detract from it and might even enhance it by expanding direct access to sources. While reliability may have to take a backseat to timeliness when using current counterinsurgency information capabilities, ICON could be designed and operated to improve *both*.

Table 7.1 shows our comparative assessment. The Mosul arrangement puts timeliness ahead of security; ICON would go further to put reliability ahead of security as well. The Mosul arrangement took important steps to integrate operational and intelligence information by bringing intelligence agents closer into the local command loop, something that ICON would strive to make seamless. Similarly, while the Mosul arrangement was an ad hoc arrangement, we believe ICON can be designed with these features in mind from the beginning.

With all the security problems bedeviling the Internet, users know that it is nevertheless superior to closed systems in providing timely and useful information of adequate quality. For this reason, we believe that a system that shifts its emphasis toward speed, inclusive access,

Table 7.1
Comparing Alternative Information Architectures

	Current Doctrine	Mosul Adaptation	ICON
First priority	Security	Timeliness	Timeliness
Second priority	Reliability	Security	Reliability
Third priority	Timeliness	Reliability	Security
Information flow	Stovepipe	Military-Intelligence integration	All operators
Adaptability	Rigid	Work-around	Flexible

and integration would meet the needs of counterinsurgency more effectively. Moreover, since building legitimacy, trust, and common purpose is the essence of successful counterinsurgency, an emphasis on information sharing would both advance and exploit this larger strategy.

Simply put, an information system designed to secure the population and improve governance cannot be a traditional intelligence system. In conventional warfare, separating intelligence and operations makes a certain sense. The enemy is beyond sight. Dedicated resources, ranging from sensors to snitches, are required to find and characterize the enemy and its movements. These resources are sophisticated and expensive. If the enemy understands how they work, their value plummets. We cannot afford many of them. The data they collect are, thus, quite sensitive. Their outputs are used to guide operations, which are typically violent and brief, leaving operators little opportunity to observe the enemy, except episodically and under highly stressful conditions. The local population is largely beside the point in such conflicts, except if unlucky to absorb the blows of war.

This model does not fit counterinsurgency well. First, it has little to do with bringing the population to our side. Second, contact between operations and the population, insurgents, and potential insurgents is deep, dense, and, thus, central in comparison to what intelligence provides. Third, winning counterinsurgency is ultimately up to indigenous forces—not just soldiers but police officers and other civil servants,

politicians, community leaders, contractors, and aid workers who traditionally never see intelligence products. Compartmentation becomes particularly harmful when such people need to work as teams. In such cases, situational awareness is anything but shared, making coordinated activity fraught with peril and misunderstanding. Worse, a team in which different members know different things cannot help but lose cohesion.

The case for inclusiveness in counterinsurgency information systems rests not only on the obvious benefits of being able to exchange information with local sources but also on the utility of improved performance on the part of local authorities and security services. Today's inadequate capabilities and limitations on sharing deprive indigenous forces of the operating advantages afforded by modern networking. Currently, Iraqi police and military troops are trying to function with information capabilities that are primitive by our standards. Yet, we expect them to substitute for U.S. soldiers and to prevail over an information-savvy foe. If most information requirements in counterinsurgency can be met by sharing with the population and other operators and users, then local security forces will be treated as indispensable allies, not as security risks.

This is not to say that traditional intelligence is utterly useless. The patient amassing of information on high-value targets cannot dispense with experts nor should it always become public knowledge. But to think that the pursuit of the insurgent leadership is the only useful activity of counterinsurgency is erroneous. In many cases, it is not even primary.

Principle 2: Build ICON to Go Native

Decisions over what information to share with indigenous forces (as well as with other allies) are likely to be the most vexing yet most important of all the architectural decisions that shape ICON. A counterinsurgency is for indigenous forces to fight and win. The more information they have the better they will have the tools to be able to do so. Beyond that, visible failure to share information with indigenous forces

signifies that those forces lack either the competence or the trustworthiness to see what U.S. forces see; it works against coalition cohesion. Finally, working with U.S. information is one way to educate indigenous forces as to how U.S. forces think about warfare; more subtly, it is one vehicle (among many) to convey how a professional military should act.

Therefore, 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 indigenous forces cannot afford the network, the United States should not stint in this matter (at $5,000 per seat, equipping a 200,000-man Iraqi Army would cost well under 1 percent of what has been spent on the war so far). The network will be open to the outside world for message exchange and external Web surfing, but including whatever content filters are required to maintain information security.

Some accommodation needs to be made for the great majority of indigenous war fighters not literate in English.[5] In the main, ICON needs to run native-language software and host services that can translate material from English into the native language on a word-for-word basis for content such as briefing charts, spreadsheets, and maps, in which verbs and prepositions are scarce and complete sentences almost nonexistent. Automatic text translation, alas, is immature and will still require human intervention: High-priority material may be directly assigned for translation, while talented individuals should be rewarded (perhaps financially) for translating material and posting medium-priority material on their own. Quasi-automatic translation of after-action reporting may be facilitated by inculcating standardized reporting formats and phrases (e.g., in the way trained personnel debrief patrols and report materials in a fairly standard way). Cross-linking text with images of events or people, GPS locations, time, etc. may be

[5] The percentage of these will depend on the location of the insurgency. English, furthermore, is many people's second language, and many indigenous war fighters will likely learn some English to work with U.S. forces adequately. If too many are simply illiterate, they may need something closer to a graphics-based point, click, and listen system.

helpful in understanding the original meaning of the text and providing context information.

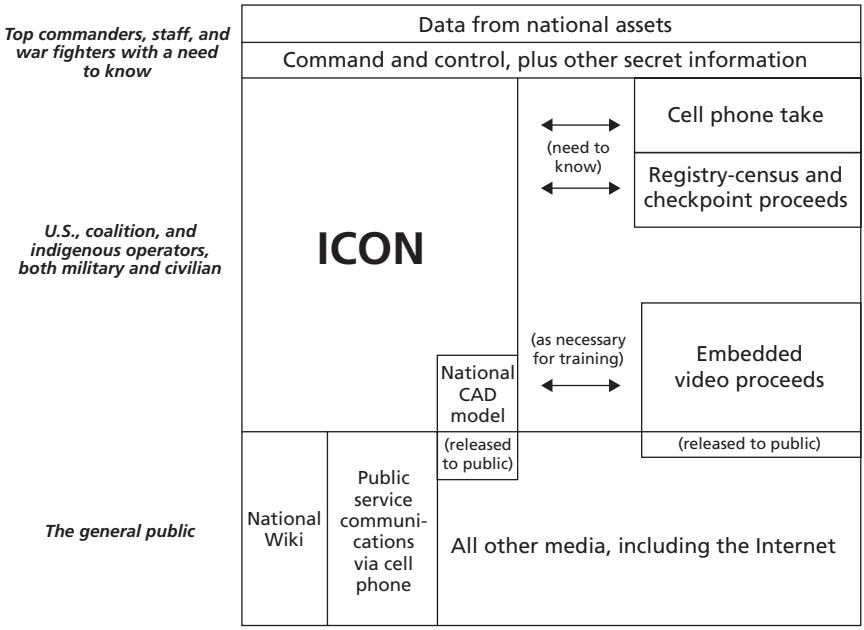
Several important networks should nevertheless be prohibitively difficult to access from an ICON client. One of them is, inevitably, highly classified material from national assets. Since such information may be useful in a counterinsurgency, some provision should be made to get it into theater, but this need not be the system that is used routinely for the myriad of counterinsurgency functions. Ironically, by limiting the distribution of such information so that it is not routinely available, U.S. commanders will be forced to develop local substitutes that can then generate material that can be more freely shared with indigenous forces.

Cell phone proceeds and sensitive census-registry data should also be restricted to protect privacy and protect the security of innocent individuals (from officials who are corrupt or acting on behalf of insurgents, militias, and others). Granted, when fighting an insurgency, such values may appear secondary, until we consider the greater consequences of exposing someone's secrets in a world in which violent death is common. Furthermore, there is a great difference between having records accessible to a few individuals within a designated intelligence cell and having records that any of several hundred thousand people can access. Easy access to great gobs of data on friends and neighbors creates a temptation best avoided.

Weapons-embedded video data should not be routinely put on the network. It is not only that storing hundreds of peta-bytes of data online is unaffordable. More important, the data are, again, personal and specific. Such video data, after all, are taken primarily for after-action review and for juridical purposes, neither of which requires everyone to access everything. Juridical purposes can be satisfied by selective posting.

Nevertheless as a general rule, and acknowledging language barriers, most of the information available to U.S. forces should be available to indigenous forces. Figure 7.1 is our notional depiction of who can access what information, arrayed from most compartmented on top to that which is open to the public on the bottom. ICON, a system broadly available to the community of counterinsurgents, sits at its core.

Figure 7.1
A Notional Access Architecture for ICON



RAND *MG595/1-7.1*

It absorbs selected information from the cell phone proceeds, the registry-census, and the embedded video, but only through a well-protected interface. Here, "need to know," which recurs throughout this figure, should be understood in its traditional sense but without adding its often unstated concomitant "someone with an appropriate U.S.-issued security clearance." Need to know means whatever is required for operators—be they from the United States, coalition partners, or the indigenous country—to do their job.

To some, this broad openness of ICON may appear naïve: Is there no information that all U.S. forces but no indigenous forces should have access to? After all, experience from Vietnam and even Iraq suggests that the loyalty of indigenous forces cannot be automatically assumed. Some may even work for the insurgency. Others may, as in Iraq, be working on behalf of one or another militia—e.g., Shiite

policemen pursue Sunnis, some of whom may actually be insurgents, with indiscriminate methods inconsistent with U.S. norms and not conducive to security in Iraq. Still others may be corrupt and might exploit adverse information on others as a reason for a "shakedown." Even those without ulterior motives may use information not to fight better, but to inform their own decision to drop out and go home. Granting these objections, separating information systems is unlikely to be the best approach to the problems and may well make matters worse. While, for instance, judgments by U.S. intelligence operatives on the quality or loyalty of indigenous forces might be the sort of material that should be in a U.S.-only compartment, stories of its existence or stories based on the material itself could easily circulate from one U.S. soldier surfing the internal Web to a friend within the indigenous force and then out to the rest of the indigenous force. Perhaps some things are best left off the network entirely.

Nevertheless, all sensitive data cannot be kept off the network, and the possibility that an indigenous soldier who sympathizes with the insurgency sees material that will flow to the other side would be quite discomfiting to U.S. commanders and war fighters. But the real problem is less one that some sensitive information may be going to the insurgents and more that some of the war fighters that U.S. forces are going into battle with carry divided loyalties.

Principle 3: Audit, Audit, Audit

For the reasons above, information security should be provided through an open regimen that places a great deal of emphasis on auditing what people do with information rather than on what information people have. Although auditing requires constant vigilance and cannot promise the kind of assurance that security compartments can, it lacks the aforementioned downsides of compartmentation. It also has the potential to detect rogue users, not merely deny information to them. By dint of being active rather than passive, it is potentially more adaptive.

The central premise is that auditing determines when an individual has or is in a position to "abuse" information, which is to say,

use it in harmful ways that differ from how a normal war fighter might use it. Because suspicious user patterns are central, identifying users reliably is sine qua non. Identification, therefore, requires that U.S. and indigenous forces access the computer system using authentication devices that link users to validated identities in a reliable way (extending the U.S. military's common access [identification] card to indigenous forces may be one such path). Audit data are not something that can be gathered offline easily (after all, it is generated from the network itself) but, for obvious reasons to be elaborated upon below, have to be tightly controlled.

Auditing techniques are complex, and many of the best tricks are either sensitive or are even more reliably secured between the ears of clever systems administrators. The following examples, however, suggest how auditing may work and what it might be able to accomplish.

Abnormal Usage

The first method is to do as credit card companies do—make note of what normal usage is and investigate deviations from that norm. The techniques will differ: Credit card companies look for spending patterns that change unexpectedly and do so by comparing baseline spending to recent spending (although certain spending patterns are per se suspicious even without a baseline)—this new pattern suggests that the recent spender is not the same person as the baseline spender. In computer auditing, we are, instead, looking for a pattern of behavior from someone who may be rogue from the outset. Here the baseline has to be a pattern of activity likely to be associated not with a specific person but with someone of a given nationality and job code. Examples of suspicious activity may be unexplained interest in the status and plans of units that are not being worked with, or attempts by someone (who does not work with intelligence issues) to see what the system "knows" about specific individuals.

Taggants

A similar technique is to slightly alter information going to selected individuals so that if it falls into the wrong hands, its path can be traced. The differences would not be so great that the information

going to one contradicts that going to another (e.g., Joe thinks the unit is going north, while everyone else thinks it is going south). Instead, wording may be different (e.g., "northerly" versus "in a northern direction") or ancillary information might differ (e.g., Joe thinks the unit has been assigned for its actions last week, while everyone else is told nothing of the sort). The next step is to intensify efforts to collect the words that insurgents are using, e.g., through signals intelligence or interrogation. To the extent that the words or rationales are specific to selected individuals, authorities can begin to zero in on such people as potential rogue actors.

Honeypots

A similar follow-up technique, used for people who may be suspicious, is to feed them information of the sort that a rogue operator may react to in a different manner than a loyal operator might. Information, directed to an individual, about a valuable but insufficiently protected target may, when passed to the enemy, cause them to take action against the target. For instance, to detect someone who is corrupt, it helps to give such an individual hints about a possible way to make money from doing something—and then watch for evidence that this person is doing or preparing to do that something.

Surveillance

Even without targeted communications, the authorities may need to keep an eye on individuals mentioned in message traffic. The sudden disappearance of an individual identified in the traffic as someone who has to be kept watch over may be a hint that someone reading the message is an advocate of more direct action than U.S. forces might have taken in similar circumstances.

Beyond the automated auditing systems discussed above are a class of systems of great use to investigators. In an insurgency, there are all too many events that might indicate an internal leak and, if left unaddressed, will only cause growing suspicion that there are bad actors using the system. Fully automated systems that flag suspicious activities are of little use when the bad actor is an authorized user and his actions are well within normal parameters, such as might be the case

of a corrupt watch officer. However, a semiautomated system can help those charged with investigating the potential misuse of the system by increasing the number of critical external events (such as a criminal act, ambush, or anything that may have been likely to have been assisted by the system) to be evaluated in the context of those who had the information and their activities. This would allow for the more routine evaluation of incidents with an eye toward understanding the potential source of either an unintentional or intentional compromise of sensitive data. For instance, the routine assessment of death and disappearance information reported by the public health department might be evaluated against who accessed information related to those people within a certain time window. Such an effort by internal security forces may assist them in prioritizing investigations and help increase confidence in the integrity of those with access to information.

Principle 4: Tune ICON to the Level of Insurgency

Insurgents tend to present themselves in one of two ways, depending on their strength relative to the government and its security forces. Each way calls for a different method of gathering information on them.

When insurgent strength is limited, they will be clandestine. Likewise, late in a successful counterinsurgency, an insurgent organization might return to being more clandestine as it seeks to hide from the more dominant security forces.

When insurgent strength grows, they 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 complex terrain. To examine how the problems differ from one another, we will briefly discuss each in turn and then how they relate to the information system necessary for the government and security forces to conduct successful actions against them.

In government-controlled areas, insurgents need to keep a low profile and mix with the local population so that they are difficult to detect, while at the same time security forces need to maintain an

appearance of normalcy to underscore the control of government and the proper functioning of society. Consequently, the information systems used to detect insurgents will need to have minimal effects on the normal population during their use, be useful in allowing for effective operations to neutralize insurgent operations, and help minimize the need for highly disruptive security operations such as cordon and searches. Such a system may seek to focus on allowing the people to contribute information voluntarily, through the use of unobtrusive collection mechanisms, as well as make it possible to allow for lower-impact security operations, such as active tailing of individuals with small teams and targeted operations. Interrogation and other similar activities that have a high potential for a negative effect on the population as a whole become the exception rather than the rule for security forces.

The system outlined in this monograph collects a great deal of information that will be quite helpful in gaining information on insurgents who are attempting to remain clandestine, while maintaining a low profile for security forces during collection. For instance, the routine use of devices configured for use in civil law enforcement activities or intelligent transportation systems (e.g., cameras, sensor nets, and vehicle tags) are extremely helpful to security organizations. These systems are nonmilitary by nature in that they were designed for other functions (such as the delivery of public management and the effective conduct of society), but they can be effectively used by the security elements tasked with finding the insurgents if the data can be accessed.[6] In addition, security elements may have a host of close-in sensor systems (such as listening devices, video systems, landline taps, and short-range signals gathering devices) that can be used within the context of their investigations and monitoring potential insurgent activity.[7]

---

[6] The insurgents might likewise make use of the system for some applications. Consequently, the security forces may wish to adopt a variety of responses, ranging from small delays in making the data available to the public to operational responses, such as deception operations and provocation operations designed to decrease the utility of such information to the insurgents.

[7] The use of the *investigation* and *monitoring,* rather then *operation,* was intentional and reflects a different sort of activity than that in which the military nominally engages. Most

In areas being actively contested by government and insurgent forces, security forces can make use of many of the same techniques and procedures used by law enforcement elements but still retain the ability to operate in areas of greater physical threat than experienced by normal law enforcement units, as well as having options of a decidedly military character, such as use of lethal force in a offensive manner. This is the arena where paramilitary police forces[8] can work best by combining their ability to operate in situations in which they might encounter heavily armed small groups but still retain their forces emphasis on protection of the public and use of police investigative procedures and intelligence processes.

The information gathering systems are still very similar to government-controlled areas, depending a great deal on the public for information and use of close-in collection actions as much as possible. However, the systems differ here because of the greater need to gather information that will immediately contribute to a public that is more vulnerable to coercion from insurgents. It is vitally important to have tools that will prevent insurgents from identifying those who are helping the government and tools that will allow government forces to rapidly respond to threats believed to be directed at the population in

---

people flagged by the system will not be insurgents or not even insurgent supporters. Rather, the targets for the investigations will turn out to be the people from whom the government is seeking to gain support and legitimacy. Consequently, security forces need to be carefully vetted, and their activities routinely audited to detect abuse. The systems discussed in this monograph become a way in which context of actions can be better assessed and lessons from investigations shared within the most interested communities. Like other law-enforcement sensitive information, this will stay in channels—in large part to protect the privacy of the innocent. Balancing "fishing" expeditions against the need to look widely for insurgents is a difficult one, and it is further complicated by internal checks to prevent misuse of the system.

[8] In this context, it is somewhat difficult to distinguish between a military force that can act like a police force and a police force that can act like a military force. A useful distinction might be one that distinguishes the two by whether the organization considers the offensive use of lethal force as a policy tool. A military force can consider this use of force as part of a nominal repertoire, while a police force would not. Both can use force, but only the military would consider offensive action as a tool to eliminate threats and shape the environment.

order to maintain its credibility with the population.[9] Offensive action combined with defenses to raise the cost of attacks would seem the best options here, and the information tools need to provide information to maximize opportunities to engage insurgents before they directly threaten the population, as well as allow responses to developing threats.

In insurgent-controlled areas, the tools to counter overt insurgents differ sharply from those required to sort insurgents out in their less visible phases; the tools are more military. The best tools available to counter clandestine organizations include routine interaction with the local population, forensic information gathering, long-term surveillance, and low-level informants. When insurgents are strong enough to be overt, such tools are either unavailable or much harder to use on a routine basis. Information shifts from the form of tips to targeted high-risk human intelligence, from close observation (perhaps with technical sensors) to a dependence on exotic remote sensors, including military systems for urban/difficult terrain operations (e.g., unmanned aerial vehicles, robots, and foot patrols). Because of the decreased ability to engage in graduated responses (say low-risk interviewing or even short-term detention for questioning), operations and, hence, the information systems needed to support the operations are of a significantly different character. Here the information systems are supporting shoot/no-shoot decisions in which use of deadly force is probable, rather than the decision to interview a potential suspect.[10] Technical systems that can help remove the ambiguity of an individual's intentions, determining whether he has hostile intent will be of great value. Technology, such as detection of weapons at a distance, combined with information on identity or group affiliation of an individual can help in deciding what to do when confronted by potential

---

[9] Always responding after the attack may only be slightly better then not responding at all if there is no effective follow-up to the attack by security forces.

[10] This points out a danger of mapping data across application domains. For instance, in countering clandestine organizations, a high confidence or reliability may be assigned to a suspect with the implied outcome being either surveillance or interviewing of the suspect. If those data were used with the tag for lethal engagement decisions, the threshold for high confidence would probably be quite different.

adversaries in a counterinsurgency environment. Such systems might be used most effectively in deliberate actions, when preparing for an assault on an area with a mix of insurgents and civilians. The systems might also help in cases in which a force is reacting to an immediate threat, say someone passing an outer perimeter, and a decision to escalate to lethal force is being made.

Principle 5: Post Before Process

Information circulation is often retarded by repeated review, a process driven by bureaucratic imperatives and an inordinate preoccupation with security. These constraints not only deprive the individual user but also contradict a fundamental requirement of successful counterinsurgency: the integration of effort across civil-military, military-intelligence, U.S.-ally, U.S.-local, and official-population lines.

Such principles as user primacy, inclusiveness, and integration prevail in the wider world of information systems by offering enormous practical rewards to individuals, enterprises, and society. These are the very principles that would permit the more effective exploitation of information in counterinsurgency and, thus, more effective counterinsurgency.

As a general rule, 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. If users find such services helpful in understanding the insurgency, they should be provided—but we believe the decision to plunge into the data or wait for the analysis should be left to the users whose training and cognition will prepare them to balance timeliness versus reliability. In other words, information should become available to operators as soon as it has been received. It should not wait until it has been thoroughly analyzed, and it should not even wait until it has been fully validated (unless raw information points too obviously to sensitive sources and methods). Should users feel uncomfortable with dealing with raw information, they can await further verification and analysis. Knowing

how to make that choice intelligently is no more than the country asks of its citizens in making intelligent political choices in today's anything-goes media environment.

Although such principles may seem obvious to denizens of Web 2.0 (a phrase coined by Tim O'Reilly to describe a world of user-provided content), they are far from prevalent in the national security community. To take just one example, the National Geospatial-Intelligence Agency used to work under the paradigm of TPED: task (satellites), process (e.g., the artifact reduction, edge conformance, and ortho-rectification of images), exploit (discerning what exactly is on the image), and disseminate. This process is often time consuming and not always transparent.

The suggested alternative uses the acronym, TPPU: task, post, process, and use. Note that "use" follows both "post" and "process," suggesting the user has a choice between the initially posted image and the subsequently processed one—or both. Still, the TPPU paradigm has hardly overtaken the TPED paradigm within the National Geospatial-Intelligence Agency or any other intelligence or information agency.

The simplest way to circulate information in today's Web-enabled world is to post it in ways that make it easy for others to find. What are needed are habits of mind, software that makes posting a virtual default option, and a system of indexing (and cross-indexing) that is logically complete and intuitive. A useful corollary feature would be to allow everyone else to append comments to the material, as is also common on the Web. To be sure, many of the comments may be irrelevant, and some may be outright wrong. But tomorrow's Web-nurtured operators should be used to these problems and, therefore, capable of recognizing and retrieving the "nuggets."

The principle of posting before processing speaks to the conduct of intelligence collection. If collectors were obligated to post information when they get it, then they would run on shorter cycles, with more immediate feedback. In essence, they would be closer to the customer but also further from their own hierarchy, since they would no longer be so dependent on higher-level approval to get material out the door. This posting arrangement would provide them one less reason to trim

their sails in favor of the hierarchy's values and norms. There would also be more corrections offered by analysts who, posting on demand, then come into possession of new or modifying knowledge. Users, Wiki-style, might offer their own perspectives via their own comments to material they see. The question of how to recognize, reward, and reinforce useful services is a hard one to answer, but it can be addressed, and the solutions are likely to make as much sense as the process that rewards or penalizes the intelligence community and its members for good or bad intelligence services.

Finally, we note that the post-before-process rule may be facilitated by encouraging the use of metadata to tag information elements so that their provenance can inform the timeliness-reliability tradeoff decisions by users that is discussed in the last principle.

Principle 6: Establish a Standard Deck and Populate It from the National Wiki

One of the essentials of conducting information gathering is a standard set of intelligence requirements (collection "deck"). It is not unreasonable for a newly arrived combat commander or police chief to want to know, for instance, what prior operations or interactions have been, who lead them, how to contact them, which local official is linked to which militias, and which insurgents are active with what tactics, and exploiting what grievances. The 160 requirements in the Appendix can be considered a prototype standard deck, one that would be modified for the local circumstances of each insurgency as well as time and place (e.g., not every insurgency has militia issues). It should be common practice to maintain an accurate and timely standard deck for every province in play, and, thus, there has to be someone assigned to maintain it—an essential, if not always exciting, task.

The responsibility for this deck, however, need not be solely vested within the intelligence community. Operators, as noted in Chapters Three and Four, have a vital role to play in adding their observations and in maintaining a history of their interactions. The elements of a

standard deck would naturally be a strong influence in developing the kind of preformatted reports discussed in these chapters.

A national Wiki, for its part, may also play a vital role in filling out the deck. First, the English-language (and ICON-restricted) version of a national Wiki would be structured in part to respond to the national deck (in other words, some of the categories would be preselected accordingly). Second, the native-language version of the national Wiki could be mined to fill out the standard deck. Third, gaps in the standard deck would be a first-order indicator of where the United States may have to throw resources into getting local citizens and authorities to contribute their expertise to the information collection. The submissions would enter a national Wiki and, thus, become available to all in the native language. Then the useful material would be translated and transferred, perhaps with additional commentary to the English-language version.

Principle 7: Rank Information by Reliability and Relevance

Inaccurate and irrelevant information is the bane of the user; nothing else so drives them away from using information systems. It might, therefore, be a useful service for ICON to have a facility by which accurate and relevant information could be noted as such so that it may float to the top of the user's mental in-box.

Unfortunately, the quest for automated or at least systemic guides to accuracy and relevance is a long-standing and oft-frustrated goal of the entire computer science profession; military users are hardly the only ones so afflicted. Several considerations make the quest particularly challenging. Reliability and relevance, for starters, are not the same. Reliability is a general property of information, while relevance is specific to the user. Furthermore, there is no easy indicator of what any

one user finds accurate or relevant—no counterpart to a "purchase," which indicates a satisfied customer in the world of e-commerce.[11]

Thus, there is no easy equivalent of amazon.com's technique in which users looking at one book are guided to other books based on what purchasers of that one book also purchased ("Customers who bought this item also bought . . ."). The best proxy for a "purchase" may be the time someone spent looking at a piece of information, but this proxy would have to be normalized for the length and difficulty of the item, and it also blurs the distinction between reading and relevance. Explicit rating systems of the sort that amazon.com offers ("3 of 6 people found the following review helpful"), or reputation systems[12] of the sort that ebay.com uses may be useful. Unfortunately, they require users to consciously annotate the material they see—something only a fraction of readers would be inclined to do at all, much less consistently. Book reviews, themselves, are useful reliability and relevance devices but an input-output ratio of books to reviews (e.g., books of hundreds of pages sell in thousands of copies versus a review of a few paragraphs or pages) does not apply to, say, message traffic. Information providers could be asked to rate the reliability and relevance of their own work, and there may be times that such self-rating might actually be useful (e.g., "Although, I am uncertain about this, I nevertheless heard . . ."). However, human nature suggests that there will be a weak correlation between the enthusiasm with which information is offered to others and its actual value. Scientific literature uses citation indexes, a more

---

[11] A "market" might be created that required that users spend green stamps (a scarce or budget-limited thing like money) for what they find accurate or relevant. The defense community uses such "funny money" all the time—often with some useful link to real money, as in the case of industrial funding. If this is the case, posters get some useful remuneration (even if only in green stamps useful for some purpose) for submitting accurate and relevant information. Conversely, such a system would discourage random reading, which is important in lateral thinking. Furthermore, micropayments (see "A Micropayment for Your Thoughts," *Wired,* [December 1, 2003]) have failed to make much headway on the Web, despite nearly ten years of advocacy.

[12] Some of the notions of reputation are discussed in U.S. Department of Defense, *Net-Centric Environment: Joint Functional Concept, Version 1.0.* (Washington, D.C.: U.S. Government Printing Office, April 7, 2005b). As of June 11, 2007: http://www.dtic.mil/futurejointwarfare/concepts/netcentric_jfc.pdf.

objective metric, as a proxy for reliability, but citations are the exception in the world of security services.

Two other methods, although quotidian, form a rather rough-and-ready guide to accuracy and relevance. One is the tendency of people to pass interesting articles around to their friends. The other is the often-exploited ability to append comments to news items and blogs. At this juncture, these informal methods may be the best reliable state of the art, and, therefore, ICON should make it easy to use these two methods (and also to experiment with generating and displaying some "eyeballs on the page" metrics) and see how far they take operators. Getting beyond that will require further research and development, a potentially worthwhile endeavor.

Results and a Caveat

The four authors examined each of the 160 requirements in the Appendix and judged whether each of them can be filled by today's information system as compared to ICON. Summing over all the judgments suggests that most of the information requirements identified in the Appendix could be satisfied and made available to counterinsurgency users if the capabilities of this and previous chapters existed. By comparison, without such capabilities only half of the requirements would be filled.[13] To be sure, the 160 information requirements were chosen because they were compatible with known collection methodologies (for instance, no question asked: identify every insurgent or detect every IED). Conversely, these estimates understate the value of ICON, because many more counterinsurgency users would have access to the additional information, thanks to the principles of inclusiveness and integration. To illustrate, if ICON disseminates twice as much useful

[13] Specifically, the four authors reviewed the 160 operational requirements and assessed whether they could be satisfied (1) with today's systems or (2) with ICON. Each author answered yes (1) or no (0), which meant that every question could have between 0 (no one thought the question could be satisfied) and 4 points (everyone thought the question could be satisfied). For the 160 requirements as whole, the average indicator for whether the information could be acquired was 3.46 with ICON, versus 1.61 without it.

information to twice as many decisionmakers—crossing military-intelligence, civil-military, international, and U.S.-local lines—the value in terms of informed decisions *and* coherent strategy—thus, in terms of improved counterinsurgency performance—could be immense.

That noted, systems cannot guard against bad decisionmaking. In deterministic systems, safety-engineering practices might be applied to guard against operator error by assuring that each step of a process be executed in a proper sequence and under the right circumstances. By contrast, the highly nondeterministic nature of counterinsurgency operations means that the processes are likely to vary so much that any system either would likely miss so much as to be useless or would actively interfere with the way operators need to use the system, given their unique circumstances. End users control their own destiny in terms of what data are presented and how those data are used. No one else is responsible for decisions made after accessing the system.

CHAPTER EIGHT

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.

Information is central to meeting such challenges. Used well, it can improve knowledge of and, thus, reduce the likelihood and effects of terrorist attacks as well as prepare all elements of counterinsurgency to proceed with a common, accurate, and continuously refreshed understanding of complex and dynamic insurgencies, specifically the whereabouts, movements, identity, and intentions of insurgents. Information can reduce the need for lethal force while improving decisions about, and precision in, its application; it can reduce particular mistakes in the use of force and limit the unintended consequences of having to use military force in general. Information can also help security forces distinguish jihadists from local insurgents, and local insurgents from

the population. It is key to redefining the struggle from one of heavy force and reciprocating violence in a perpetual war of attrition to one of competing truth and a more promising contest of cognition. Information transparency puts pressure on a government to respond to its citizens' needs by enabling citizens to express themselves about their community and their country. It can thereby improve the performance and accountability of local security services, facilitate their cooperation with the population, and reduce reliance on foreign forces.

Yet, reports from Iraq and Afghanistan suggest that there is a great deal of information of relevance to counterinsurgency that could be, but is not, collected or, if collected, is not made available to those who need it. It is almost as if the U.S. defense establishment had assumed that information had a decisive role to play only in major warfare. Clearly, counterinsurgents should tackle the challenges of gathering, disseminating, and using information in a radically different way than they are doing.

This basic finding matches the results of research recently done at the National Defense University concerning the exploitation of information power in stability operations (which are similar to, if less hostile than, the conditions of counterinsurgency). That work "concludes that utilizing the elements of the information revolution in a strategic approach to stability operations would have positive results." It prescribes that the U.S. government place a high priority on integrated civil-military exploitation of key commercial information technologies; that the focus be on enhancing the host nation's governmental, societal, and economic development; and that data-sharing agreements be reached with all "regular participants" in such operations (e.g., the UN). Those recommendations are compatible with our study's proposals to make greater use of information technology and information itself in counterinsurgency.[1]

---

[1] Franklin D. Kramer, Larry Wentz, and Stuart Starr, *I-Power: The Information Revolution and Stability Operations* (Washington, D.C.: Center for Technology and National Security Policy, National Defense University, Defense Horizons Paper No. 55, February 2007), p. 1.

Summary

Having analyzed a representative, although not comprehensive, list of information requirements (see Chapter Two and the Appendix), we learned that counterinsurgency demands a large amount of exceptionally diverse information. This information is different, more eclectic, more nuanced, more textured, and more complicated than the information normally required for regular combat between two opposing forces. Because the information needs of counterinsurgency users are so vast, varied, and unpredictable, limitations on inclusiveness carry a high cost. Even during a security operation, the information needed for counterinsurgency is as much or more about context, population, and perceptions as it is about the hostile force. We also find that only a small fraction of the information needed would likely be secret information gathered by secret means from secret sources, thus putting a very different light on the need for information security (an issue to which we will return).

Although timeliness, we learn, is critical, not only in clearly hostile situations but also in ambiguous ones, it cannot come at the expense of the reliability of the information. Counterinsurgency mistakes—such as those involving deadly force, wrongful detention, gratuitous intimidation, and humiliation—have especially harmful consequences. At the same time, we have found that reliability does not necessarily require vertical controls, exclusion, and compartmentalization. Given the main sources of information—local people and other users of the same information—there is little or no advantage in having information hierarchies sift, sort, analyze, and otherwise "process" information—all of which take precious time. Moreover, ICON is designed to allow and assist every user to be an analyst—a *thinking* user. As all Internet participants know, user-driven networking dramatically reduces the struggle of getting and sharing information, but it does not enable us to use that information with no need to reason. Quite the contrary, by enabling users to seek and get the information they need, networks designed to serve them make them better analysts. This effect is not only possible in counterinsurgency, by creating ICON, it is vital to success against networked and elusive adversaries.

Of the information required for counterinsurgency operations, according to our analysis, less than 85 percent has to come from traditional intelligence collection.[2] Fortunately, the opportunities for gathering "open-source" information are great, *if* counterinsurgents interact with the local population, which they should do in any case. Thus, information sourcing can be approached with much greater ambition; requirements need not be confined to what intelligence sources might yield. Instead, requirements can encompass the demands of users for any and all data that may bear on any aspect of either long-term counterinsurgency campaigns or episodic security operations. More than 80 percent can probably be found in one of two major sources: the population and counterinsurgency operators (to include those outside the military) themselves. Our study has developed techniques that can facilitate the collection of such information (e.g., through preformatted reports conveyed via cell phone) and its distribution via ICON. We have also explored other potential sources of information.

Census and National ID Cards

Effective governance depends on knowing the population, demographically and individually. Eligibility for government services should be fairly and fully established. Enabling persons to identify themselves and one another can contribute to confidence. While these identification methods are not foolproof, they can also help security services to enforce the law and apprehend terrorists with reduced risk of mistake.

Cell Phones

Encouraging the ownership and use of cell phones throughout the population would provide valuable and valued connectivity between citizen and citizen, citizen and government, citizen and the outside world. It could also be useful to engineer cell phone systems to make it easier to identify individuals and their whereabouts, which would aid in delivering government services and in counterinsurgency operations.

---

[2] We certainly do not mean to diminish the importance of normal intelligence gathering, be it technical or human, in counterinsurgency. But we do wish to point out its inadequacy.

Embedded Video

Recording instances of violence would help in identifying perpetrators, in holding security services accountable, and in ensuring judicial fairness. It would also help correct misinformation about counterinsurgency abuse that insurgents can use to undermine government legitimacy.

National Wiki

The opportunity for the population to tell about and learn about their circumstances, their country, and their concerns, unencumbered by sect or tribe, would increase their sense of individuality and citizenship as well as provide valued information for operations.

ICON

Regarding ICON, the information system designed to house and disseminate the information required for conducting counterinsurgency, we rapidly conclude that its most important requirement is user primacy, a necessity if users are given the responsibility and the training to solve the difficult war-fighting problems that they encounter day to day. From user primacy follows two related requirements: inclusiveness and integration—not only immediate access to any knowledge accessible via the network but also the unhindered ability of users to collaborate as peers. These elements are especially vital in counterinsurgency, which must be collaborative to succeed. The ability to cross organizational and international boundaries to coordinate action and to get information is a sine qua non. This requirement for connectivity extends not only across services, agencies, and coalition nations but also to local authorities, security services, and citizens—and because it cannot be scripted in advance, ICON must permit ad hoc collaboration. Integration also helps to ensure that users get information from the rest of the user community, which is a primary source.

Naturally, 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 systems, 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.

ICON will need to be managed, not controlled. Network management should consist of essential services only: technical help, standards, updating for new systems and applications, and the facility for security blocks. Although ICON will be used by all who are involved in counterinsurgency (as well as some interlopers), it would need to be managed by the United States. Unlike traditional military and intelligence networks, managing ICON does not mean controlling the information that courses through it or control over the users who have access to it—which is a radical shift in the U.S. security establishment's culture.

ICON is best viewed more as a utility service than as a system. It provides a capability to all those involved in a counterinsurgency campaign—international and local, civil and military. It has to be built to be left behind as a capability for the local government, its security forces, and the people they serve. Even when the embers of insurgency have died out, the society's ability to share information and collaborate can contribute to both the legitimacy and effectiveness of the state, thus depriving any future insurgency of the alienation that it needs to grow.

Governance, Accountability, and Public Expression

Although the specific information-collection capabilities we propose—the registry-census, the cell phone proceeds, national Wikis, and CAD models—are designed to support security operations, they can also be used as important components of governance, accountability, and

voice. 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. Wikis can be adapted to permit citizens to talk with or write to their government about services. These capabilities are truly dual-use investments.

By such means, society as a whole approaches the information age faster. Historically, information technologies have been associated with dystopias, such as that portrayed in *1984*. But from roughly the early 1980s on, an influential body of thinking[3] has argued that information technologies are not only compatible with freedom, they encourage it. Everything else being equal, a country armed with information technology and the Internet will have an easier time adopting Western political mores than those without. Literacy will be encouraged, there will be a wider range of material to think about, communications will be freer, and peer-to-peer information will flow more horizontally.

We are not so naïve to pretend that the transition will be effortless and automatic: China, still authoritarian, has over a hundred million Internet users. Nor do we advocate that, when the United States helps a country defend itself against an insurgency, the first thing it should do is to bring the country up to U.S. standards in digitization; it is unaffordable and requires many other prerequisites (e.g., literacy, electricity, and systems administration skills). Furthermore, as we have recognized here, third-world countries are more apt to enter the digital age via cell phone rather than via desktop.

Nevertheless, as a general rule, and in the long run, anything that encourages the accelerated adoption of information technology serves U.S. goals. The specific capabilities proposed here are, however, directly conducive to good governance and hence the kind of legitimacy that helps counter insurgency.

Start with governance. At a minimum, every functioning government has to know whom it is governing. The registry-census provides this information. By inquiring not only about who is living where, but their housing, employment, and health status, a government gets a

---

[3] See, for example, Ithiel de Sola Pool, *Technologies of Freedom* (New York: Belknap Press, 1983); Peter Huber, *Orwell's Revenge* (New York: Free Press, 1994).

well-rounded picture of its citizenry, an essential prerequisite to supplying basic social services in a fair and efficient manner. The cell phone system's public safety features make it easier for local and national authorities to respond to trouble, whether man-made, accidental, or otherwise, another important aspect of governance. The national CAD model can facilitate the delivery of public services, safety, and city planning.

Accountability is another important benefit of the capabilities mentioned. The tracking of how well government officials respond to citizens has been mentioned. Cell phones can also be used to transform the delivery of basic services, reducing the amount of annoying information requested and creating a basis for monitoring the efficacy of service delivery. A national Wiki, as noted, can easily be a forum through which citizens can indicate problems in their neighborhood and a vehicle by which the government can record that they have been addressed—or a vehicle by which citizens can remind the government that they have not been addressed or, at least, not very well addressed. Embedded cameras are a way of ensuring some degree of circumspection among security services, lest their misdeeds find their way into public archives. Also, the audit capabilities of ICON may persuade rogue operators within the indigenous government to act with discretion.

Giving the people a voice is a third benefit. At its most elementary level, a voice is acquired by a citizen telling the government that he or she exists. Elementary as it might seem, being enumerated is the first step in being counted. Being asked after comes a close second. The ability to summon the government—by cell phone or via a national Wiki—never hurts either. A national Wiki, if well-used, allows citizen not only to proclaim their individuality but to write their opinions of their community into the public spaces. None of these services will ensure that citizens do not see themselves primarily as members of communities in which they had no choice, such as their clan, tribe, or ethnic group. But they do provide a basis for self-assertion, at least vis-à-vis the government.

The wisdom of collecting enough data on a nation's citizens to the point at which each one can be characterized individually may sound

somewhere between mundane (credit card agencies do this routinely in the United States) and Orwellian. But collecting data is an indispensable first step toward a philosophy of governance—all too absent in the developing world—that treats the state as a servant of the people rather than the people's master. Whether or not a government is democratic or autocratic, a widespread feeling among the people that their presence has not gone unnoticed and their needs have not gone unrecorded—in which *their* connotes ownership as much as assignment—precedes the formation of loyalties that bring the citizens toward the government's side.

Adapting Information Capabilities to the Scope and Locus of the Insurgency

Unfortunately, many of the capabilities discussed are hard to carry out under conditions of deep insurgency—e.g., where police officers have to make greater efforts to hide their identity than insurgents do. This is particularly true for the national registry-census and the provision of identification cards, but deep insurgency may also affect other services, such as the provision of cell phone capabilities (e.g., because of damage to infrastructure) or the ability to respond to 911-like calls.

Thus, exactly which of the various recommendations will work and at what cost, broadly understood, have a great deal to do with how developed the country's economy is and how intense the insurgency is (they also depend on culture-specific factors). A middle-income country with a low-level insurgency may provide the best circumstances for collecting information, because of higher levels of cell phone and computer ownership, greater urbanization, more people who can operate and maintain high-technology equipment, a reasonable chance for some efficient records collection, a capacity for digitization (e.g., for ID cards). However, civil liberties issues may be raised because privacy tends to be more respected in such a country and the threat may not be high enough to persuade people to tolerate data intrusiveness. Although a hotter insurgency may push such constraints to the background, it may also make certain types of data collection more difficult

to carry out. The greater risk of conflict in urban areas raises the importance of the national CAD model (e.g., because of fields of fire and conflict within buildings) and may lead to a more interesting, but not necessarily more reliable, national Wiki. Matters that merit attention in conflict in urban areas include the rapid recovery of the cell phone service after periodic attacks, countering sophisticated evasion of identification systems, and greater familiarity with video. Conversely, in a country with low incomes and a simmering but not burning insurgency, electronics are likely to be scarcer, record keeping more haphazard, and the civil service less efficient (with exceptions, e.g., India) and more corrupt. Finally, lower-income countries, especially those with rural insurgencies, are the toughest environment for the information-rich approach, even if the citizenry should grasp the opportunity for cell phones eagerly and will have limited objections to privacy invasions. The national CAD model will have less relevance, and a national Wiki may have a harder time getting off the ground (people will still be getting used to cell phones). Rapid urbanization, especially if driven by violence, will force periodic revisits of the registry-census. Keeping electronics in good repair will be harder.

Hence the irony: Many of the most promising counterinsurgency capabilities have to be implemented *before* an insurgency takes place, or at least before it has gathered a head of steam.[4] Determining when a country will fall into an insurgency is not so easy (redolent of the punch line: just watch where I get off the bus and depart the stop before mine). But another approach is to support, encourage, and even help fund capabilities in large parts of the world in which the United States has an interest and which may be prone to insurgency, but in which adequate standards of law and order can be said to prevail. For a fraction of the cost of prosecuting today's insurgencies, might it not be possible to improve the governance of large and potentially trou-

[4] However, many of the proposed surveillance features of the cell phone system would be deemed unacceptable if the country is *not* being threatened by an insurgency. One approach may be to adopt these features but establish tight procedural prohibitions against accessing such information (e.g., the equivalent, in the U.S. context, of requiring a search warrant).

blesome swaths of the world before such improvement becomes both absolutely necessary and prohibitively difficult?

Implementation

No breakthroughs in information science or massive investments in network infrastructure are required to improve information capabilities for counterinsurgency. Many good technologies—high-speed storage and retrieval, information search, collaborative tools, and software agents—are being propelled by the Internet. Others—wireless connectivity and switching, handheld access, and support for heterogeneous environments—are coming from the telecommunications sector. Although the national-security market is too small to develop such technologies for its own use, it is large enough to ensure that they can be adapted for counterinsurgency.[5] Overall, the armed services are gradually getting better at adapting commercial information technology (IT). Slow progress is also being made in adapting military culture, structures, and concepts of operations to exploit that IT. DoD already has a communications and services backbone, the Global Information Grid, to support worldwide military operations, and it can be extended to any theater in which U.S. services and agencies find themselves. Nearly all potential ICON users—U.S. forces and others—either possess or can quickly acquire requisite technical skills to utilize the services that these technologies and infrastructure offer. The swift global spread of the Internet has proven that humans are quickly learning how to use networked information as a utility, without having to know how it works. In addition, prices of access—devices, media, and services—are declining rapidly because of wider economic forces. Future enhancements and needed skills will be available from general markets

[5] The transformation of U.S. forces begun some years ago to exploit information networking in expeditionary warfare, noted earlier, has involved increased reliance on and investment in advanced command, control, communications, computing, intelligence, reconnaissance, surveillance, and target acquisition, including the formation of a Global Information Grid, the purpose of which is to provide information to and permit collaboration among U.S. forces operating worldwide.

and usage. There is, in other words, a foundation of technology and infrastructure on which to build.

Can the U.S. government procure ICON as a specified procurement of a system? The record is not encouraging. Reliance on normal government procurement processes would guarantee that the principles of ICON would not be met any time soon. DoD traditionally turns to defense contractors ("lead systems integrators") to buy and assemble information solutions, in part because red tape discourages commercial 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 DoD information networks.

Out of frustration, users and the combatant commands that represent them have taken matters into their own hands—buying and jury-rigging solutions, not least of which is making an ad hoc migration toward the Internet. This model is hardly the worst; not least because it spurs the early rejection of bad ideas. Will such a market mechanism work for ICON? The answer is yes—to some extent. Insofar as insurgencies continue to demand that governments and their international supporters (1) strive to increase their effectiveness and legitimacy and (2) understand the importance of information power to these ends, there will be a demand for the capabilities of ICON. This demand will attract providers, infrastructure, and technology—up to a point. It cannot be assumed that governments and populations facing insurgency will have sufficient resources and skills to connect. Therefore, foreign-aid resources may be needed to finance the devices for and the participation and training of local users. Some special, non-Internet, features of ICON are not likely to be readily developed according to user demands, especially the ability to secure what truly must be secured and to do so as and when needed. Finally, some system of standards and process of certification will be needed.

If the U.S. government does not act or if it acts according to existing procedures, ICON and the other capabilities proposed here will not be available soon enough or broadly enough to combat the growing threat of complex and dynamic insurgency. The wisest first step the

government could take to realize ICON is to call together counterinsurgency information users and technology providers (the real ones!) in a free-form discussion of how to proceed. For now, the authors encourage the government to think of providing a limited, but critical, role in convening users and providers; conducting selective research and development; suggesting standards; and engaging foreign partners.

Research and Development Needs

Although research, development, and engineering of some sort will be needed, no "blue-sky" program is called for. Specifically, we suggest the following:

- 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

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 dynamic that drive

it all. It has led the way in creating a global information infrastructure. Its technology and service providers have shown remarkable creativity and sensitivity to user needs. While the U.S. national security establishment has been a straggler for the last two decades or so, it is beginning to find its stride in applying information technology and network principles to warfare, and it is attempting to remove bureaucratic, cultural, and regulatory obstacles to doing so.[6]

Gaining advantage on the information level of counterinsurgency is possible, but it will take focus, commitment, and cultural-institutional transformation. By stressing that the technology and infrastructure largely exists, we do not mean to suggest that developing the information capabilities proposed here will be easy. The required financial investment is nontrivial, though not large when compared with what the United States is spending to prevail over insurgencies in Iraq and Afghanistan. More formidable are the system engineering and management demands.[7] (The Defense Department is still working on a process to govern the evolution of the Global Information Grid, which would be the basis of ICON.) At the same time, the development of ICON and associated information-gathering capabilities for counterinsurgency should not be "over-determined" or tightly controlled by government. In any case, the engineering and management obstacles that need to be overcome are surely not beyond the country's abilities.

The United States has a history of marshalling its technological power to fulfill strategic needs—e.g., to prevail in World War II and the Cold War. It now faces a threat to national and international security that seems to have confounded its security establishment, begging the question: How can the United States use its strengths and advantages in information networking to solve this problem? The authors hope that this study has provided some answers, as well as some hope.

---

[6] Including initiatives to give Title X acquisition authority to the joint organizations that best represent military user needs.

[7] The best treatment of such demands in the context of the Global Information Grid is by Jeremy Kaplan, *A New Conceptual Framework for Net-Centric, Enterprise-Wide, System-of-Systems Engineering* (Washington, D.C.: Center for Technology and National Security Policy, National Defense University, Defense & Technology Paper No. 30, July 2006).

APPENDIX

Disaggregated Information Requirements

This appendix lays out 160 identified requirements to support military operations in a counterinsurgency. In Table A.1, the second column is a shorthand description of the requirement. Requirements followed by an asterisk are those that the four authors collectively felt could be significantly better filled with the novel information sources and ICON parameters discussed in the main text.

The next column, source, represents the judgment of the four authors on from where the information to satisfy the requirements should come. Our basic choices where three: from the intelligence community (including those embedded within combat units), from operators (based, in part, on what they observe), and directly from the population (e.g., through census surveys or volunteering the information). In some cases, a mix of approaches was indicated.

The last three columns—timeliness, reliability, and security—represent our judgment on the relative importance of these three features for each requirement. In general, "1" means most important, and "3" means least important. Specifically, for timeliness, urgent is "1," time sensitive is "2," and not time sensitive is "3." For reliability, a "1" means the information has to be highly reliable; a "2" means that it should be evaluated for reliability by experts; and a "3" means only that the information should be pertinent. For security, "1" means that the information should be restricted to U.S. forces; a "2" means that it can also be shared with coalition forces; and a "3" means that it can be publicly distributed.

Table A.1
Information Requirements

No.	Requirement	Source	Timeliness	Reliability	Security
1	How many insurgents are there? What capabilities? What tactics? How skilled, motivated?	intelligence	2	1	2
2	Has the number of insurgents grown in the area? Why? How much?*	population	2	1	2
3	What is the composition of indigenous forces operating with U.S. forces?	intelligence/ operations	2	2	2
4	Will operation be mechanized, on foot, armored, or a combination thereof? Implications of each?	intelligence/ operations	2	1	2
5	What is the economic condition of the general population and how has it changed? Food, water, utilities, communications?*	population	3	2	3
6	What is unemployment level for young males?*	population	2	3	3
7	What is the most pressing economic need for the area?*	population	3	3	3
8	What is the most important near-term infrastructure/economic improvement that a small counterintelligence unit can effect?*	population	3	2	2
9	Who will lead a combined operation? Is the indigenous force well led?	intelligence/ operations	2	3	2
10	Has the indigenous force been apprised of your force's pending arrival? (friendly fire)*	operations	2	1	2
11	Is the indigenous force accompanying the U.S. force using with same COIN ROE?*	operations	1	1	2
12	Does the indigenous force have the same ROE?*	operations	2	1	2
13	If not, does the indigenous force know the U.S. ROE?*	operations	2	1	2
14	Has the indigenous force operated or trained with U.S. forces?*	operations	2	2	2

Table A.1—Continued

No.	Requirement	Source	Timeliness	Reliability	Security
15	For what duration would indigenous forces from other towns/provinces be available?	intelligence/ operations	2	2	2
16	Status and location of simultaneous indigenous-force operations in unit's AO*	operations	1	1	2
17	What experience does the indigenous force have?*	operations	2	1	2
18	Are there ongoing operations by indigenous security forces? What success have they had?*	operations	1	1	2
19	What to expect at the indigenous force location?*	operations	2	1	2
20	What measures have government local forces taken to preclude insurgent growth from outside?*	intelligence/ operations	1	2	2
21	Willingness/ability of the indigenous force to defuse the impact of civilian casualties*	operations	1	1	2
22	What are the loyalties of those involved? Government, tribe/clan/family, sect?*	intelligence	2	1	2
23	Is the local indigenous force infiltrated by insurgents?*	intelligence	1	1	2
24	Can one distinguish between security forces and insurgents dressed in their garb?*	population	1	1	2
25	Is there a presence of "death" squads?*	population	2	1	2
26	What current tactical info should be transmitted to indigenous units?*	population	2	1	2
27	How stable is the local government?*	population	2	1	3
28	How legitimate is the local government?*	population	2	1	3
29	How effective is the local government?*	population	3	2	3
30	How trustworthy is the local government?*	population	2	1	2
31	What are the location and current contact info for local government leaders*	population	2	2	2

Table A.1—Continued

No.	Requirement	Source	Timeliness	Reliability	Security
32	Is the local government attempting to intervene during/after hostile actions? (U.S. side/insurgent side?)	population	1	1	2
33	What is the feasibility of the town leadership supporting searches for weapons/ordnance cache(s)?	population	2	2	2
34	What is the feasibility of the town leadership supporting searches for insurgents?	population	2	1	2
35	Who are the wealthy families?	population	2	3	2
36	What tribe/clan/family is predominant?*	population	2	3	3
37	Are there any longstanding family/clan/tribe feuds?*	population	2	3	3
38	Which sect appears to be the aggressor?*	population	1	1	3
39	What is the relationship between the sect/tribe/clan/family and the insurgency?*	population	2	2	2
40	What is attitude held by citizens toward insurgents? Fear, admiration, both, neither?	population	2	3	3
41	If insurgents provide neighborhood services, how would locals react to their being captured or killed?	population	2	1	2
42	Are the insurgents native to this area?	population	2	2	3
43	Are there foreign insurgents?	population	2	1	2
44	Do local insurgents conduct operations outside of this area?	intelligence/operations	2	1	2
45	Is religious extremism a factor?*	population	2	2	2
46	Are local religious officials attempting to intervene during/after hostile action? (U.S. side or insurgent side?)*	population	1	1	2
47	What contractor(s) are present?*	operations	2	2	2
48	What are the contractor points of contact in the town or village?*	operations	2	2	2

Table A.1—Continued

No.	Requirement	Source	Timeliness	Reliability	Security
49	What OGAs have presence in the area of operation?	operations	2	1	2
50	What have contractors done and how successful were they?*	operations	2	2	2
51	For how long have contractors been there?*	operations	2	2	2
52	For how long have OGAs been there? Doing what?	intelligence/ operations	2	1	2
53	Do OGAs change/switch personnel in the town or village on a regular basis?	intelligence/ operations	2	1	1
54	What is attitude held by citizens toward contractors?*	population	2	2	2
55	What is nature/status of OGA personnel's relationship with town/village leadership and citizens?	operations	2	1	2
56	Can OGAs act as interlocutors with town/ village leadership?*	operations	1	1	2
57	Previous injuries/threats to contractors? Details and locations?	operations	2	2	2
58	Is the indigenous population hired for work?*	operations/ population	2	2	2
59	Are there women in contractor companies?*	operations/ population	2	2	2
60	Are there women in OGAs who work directly with local women; if so, doing what?	operations	2	1	2
61	What have OGAs enjoyed the most success in doing recently; did the success put them in good stead with locals?	operations	2	2	2
62	Have contractors worked with/cooperated with COIN forces?*	operations	2	1	2
63	What lessons can be learned from contractors?*	operations	2	1	2
64	Have COIN forces worked with OGAs in the past?	operations	2	1	2

Table A.1—Continued

No.	Requirement	Source	Timeliness	Reliability	Security
65	Would/can contractor(s) defuse COIN force operations viewed as destructive by locals?*	operations	2	1	2
66	Can OGAs provide tactical support to COIN operations?	operations	1	1	2
67	What can contractors do to assist COIN forces?*	operations	2	1	2
68	Do OGAs have communication (open/secure) with COIN forces?	operations	1	1	2
69	What communication links exist between COIN and contractors?*	operations	2	1	2
70	Have insurgents worked with/cooperated with contractor(s)?*	operations	2	1	2
71	How trustworthy are contractor(s)?	operations	2	1	2
72	Do NGOs work in area? For how long? What do they do?*	operations	2	3	3
73	How have NGOs been accepted?*	population	2	3	3
74	What can NGOs do to assist (peripherally) COIN? (intelligence/contacts)?	operations	2	2	2
75	Do the NGOs reside in the area of operation?*	operations	1	3	3
76	Can/will NGOs in the AO play a role in defusing the impact of civilian casualties?	operations	2	2	2
77	Has there been religious tension?	population	2	2	3
78	Have religious insults taken place? (For example, damage to mosques, religious leaders killed?)	population	2	2	3
79	What mosques are there? What shrines? What schools? What hospitals?	population	3	3	3
80	What is the cultural status of women in the AO?*	population	3	3	3
81	What effect has women's status had on the local population? For example, widened the gap between the sects?	population	2	2	3

Table A.1—Continued

No.	Requirement	Source	Timeliness	Reliability	Security
82	Are insurgents led by religious figure(s)?*	population	2	2	3
83	Will COIN be conducted by combined U.S. and indigenous forces?	operations	2	3	2
84	How flexible are ROEs? How much authority does the U.S. counterintelligence force have to change ROEs?	operations	2	1	2
85	Are U.S. and indigenous communications compatible?	operations	1	2	2
86	What are the ingress/egress routes in the AO?	operations	2	1	2
87	What are the high points/vantage points in the city/AO?*	operations	2	3	2
88	Are maps up to date? City maps accurate (to avoid dead ends and other tactically dangerous positions)? Maps concur with overhead satellite photos?*	operations	2	2	2
89	Can the AO be encircled?*	operations	3	1	2
90	Is the population in town separated by clan/tribe/sect?*	operations/ population	2	1	3
91	What is the feasibility of splitting the force during operations in response to a change in the tactical environment?*	operations	2	1	2
92	How small a force must remain intact for self-protection?*	operations	2	1	2
93	How much of the town needs to be taken to gain and retain a foothold?	operations	2	1	2
94	Where is the most vulnerable point of entry?	operations	2	1	2
95	What are the locations of insurgent headquarters, lay-up points, and staging areas?	intelligence	2	1	2
96	What is the local insurgency's means of logistical support?	intelligence/ population	2	2	2
97	Where are the nearest known reinforcements for insurgents?	intelligence	2	2	2

Table A.1—Continued

No.	Requirement	Source	Timeliness	Reliability	Security
98	Who controls town ingress/egress?*	population	2	1	2
99	What is the current viability of originally planned egress route(s)?	population	1	1	2
100	Can the local population travel in/out of town freely or is it restricted to the sect in power?*	population	2	2	3
101	Are insurgents evenly distributed throughout the area or in control of specific portions of the area?*	operations/ population	2	1	2
102	Is the security perimeter secure and holding?	operations	1	1	2
103	What are the lay-up point(s) within the perimeter to be used after hostile action?*	operations	1	1	2
104	If the indigenous force's mission requires assistance, what are the preferred route(s) to the indigenous force?*	operations	1	1	2
105	How to get ongoing tactical environment updates?*	operations	1	1	2
106	Would contractor personnel be required to depart prior to COIN operations and under what circumstances?*	operations	2	1	2
107	Would OGA personnel be required to depart prior to COIN operations and under what circumstances?	operations	2	1	2
108	Do contractors have near real-time information on COIN force locations and activities (e.g., roadblocks)?*	operations	2	1	2
109	Do COIN forces have near real-time info on OGA personnel locations and general activities?	operations	1	1	2
110	Do OGA personnel have escape/evasion plans? What are they?	operations	1	1	2
111	Do contractors have ground transportation?*	operations	1	1	2
112	In mixed-sect urban areas, how to identify the source of hostile fire/ambushes?*	operations/ population	1	1	2

Table A.1—Continued

No.	Requirement	Source	Timeliness	Reliability	Security
113	Prior to commencing combat operations, how to determine if the force in question is an insurgent unit?	population	1	1	2
114	How to determine if hasty detours have been established by unknown persons?	population	1	2	2
115	Is there any suspicious movement at or near the security perimeter?	operations	1	2	2
116	How to determine the reason(s) for a controlled retreat by insurgents (are they losing, setting an ambush)?*	operations	1	2	2
117	How to determine the intent of an ambush/hostile fire by a smaller-than-usual insurgent force (i.e., 2 to 4 insurgents)?*	operations	1	1	2
118	How to track the movement of all people/vehicles during hours of darkness (as feasible)?*	operations	2	2	2
119	What is the status of friendly KIA/MIA indigenous-force location?*	operations	1	1	2
120	Are insurgents holding prisoners? How many?*	intelligence/population	3	1	2
121	How to determine number of insurgents killed/captured during an operation and the ratio to any U.S.-caused civilian casualties during the same operation (i.e., was it worth it)?*	operations	2	2	2
122	How to identify KIA/MIA who are not innocent civilians (probably a bridge too far)?	population	2	2	2
123	How to identify local officials or family for returning the remains of local citizens who were killed?*	operations/population	2	1	2
124	How much time has elapsed since the last COIN operations in the area?*	intelligence/operations	2	3	3
125	What operations have been conducted by the insurgency over the past 6 months?*	operations	2	2	2

Table A.1—Continued

No.	Requirement	Source	Timeliness	Reliability	Security
126	Who is the point of contact from the last operation?*	operations	2	2	2
127	What lessons can be learned from those contacts?*	operations	1	2	2
128	Are there lessons to be learned from analogous COIN operations?*	operations	1	1	2
129	Has the town ever been taken by a prior counterintelligence force?*	operations	3	2	3
130	What size of force/intensity of combat operations was required by government/ indigenous to gain/retain control of an area?*	operations	2	2	2
131	Did the insurgents fight or evacuate the town?	operations	3	2	3
132	Have insurgents taken control of nearby a town? What methods were used to gain control?*	intelligence	1	1	2
133	What worked? What did not work?	operations	1	2	2
134	Why is there a need for renewed operations?*	intelligence/ operations	2	2	2
135	Have there been changes in the tactical environment since the last operation?*	operations	1	2	2
136	Do insurgents control hospitals/medical facilities?*	population	2	2	3
137	What is the frequency of suicide bombs/ IEDs?*	operations	2	2	2
138	Has the local insurgency morphed? In what way? Weapons? Operations? Organizations?*	population	2	1	2
139	Do tribes/clans/families dress differently?*	population	2	3	3
140	Are insurgents embedded geographically, demographically, socially, or by appearance?*	population	2	1	3
141	Are there many English speakers among the population?*	population	3	3	2

Table A.1—Continued

No.	Requirement	Source	Timeliness	Reliability	Security
142	Do community leaders need interpreters?*	population	2	3	2
143	What impact could the phase of the moon, the day of the week, or holidays have on counterintelligence ops?*	operations	2	3	2
144	What is the capability of validating citizen ID?*	operations	2	1	2
145	at checkpoints?*	operations	2	1	2
146	during confrontations?*	operations/ population	1	1	2
147	at other required times?*	operations/ population	3	2	2
148	What is the status of medical evacuations?*	population	1	1	2
149	What is the inventory of COIN force ammo/ordnance subsequent to combat operations?*	population	1	3	2
150	If cache(s) are discovered, what is the feasibility of destroying them in place?*	population	2	2	2
151	What is the feasibility of securing caches until additional means of moving ordnance arrive?*	population	2	2	2
152	How to immediately interrogate captured insurgents for real-time/near real-time info (e.g., local insurgent lay-up locations)?*	intelligence	1	1	2
153	Is there any ongoing air support being employed by the indigenous force?*	operations	2	1	2
154	What is the status of the COIN force KIA/ MIA?*	operations	1	2	2
155	Is air support employing laser-guided munitions?*	operations	2	1	2
156	How to maintaining contact with prepositioned counterintelligence snipers?*	operations	2	1	2

Table A.1—Continued

No.	Requirement	Source	Timeliness	Reliability	Security
157	Are snipers effective? What are the results?*	operations	2	1	2
158	Can snipers provide real-time info on the tactical situation? What kind?*	operations	1	1	2
159	What constitutes tactical control of a village/town (in the near term)?*	operations	2	1	2
160	How long will U.S. counterintelligence forces remain in the community?*	operations	2	2	1

NOTES: Timeliness, reliability, and security represent the authors' judgment on the relative importance of these three features for every requirement. Requirements followed by an asterisk are those that the four authors collectively felt could be significantly better filled with the novel information sources and ICON parameters discussed in the main text. In general, "1" means most critical, and "3" least critical. KIA/MIA: killed in action/missing in action. COIN: counterinsurgency. AO: area of operations. OGA: other government agency. ROEs = rules of engagement.

Bibliography

Alberts, David S., and Richard E. Hayes. *Power to the Edge.* Washington, D.C.: Command and Control Research Program (CCRP), Office of the Assistant Secretary of Defense, 2003.

Block, Ryan. Live from Macworld 2007: Steve Jobs Keynote. *Engadget,* posted January 9, 2007: http://www.engadget.com/2007/01/09/live-from-macworld-2007-steve-jobs-keynote/

de Sola Pool, Ithiel. *Technologies of Freedom*. New York: Belknap Press, 1983.

Focus on Advocacy & Advancement of International Relations, LLC. "Iraq's 2003 Official Census by Ministries of Trade and Planning for the Food Coupon Distribution for the UN Oil-for-Food Program." Washington D.C., 2003. As of June 11, 2007: http://web.archive.org/web/20040615113507/http://www.faair.org/images/Iraq-Census-Total-2003.pdf

Galula, David. *Counter-Insurgency Warfare: Theory and Practice.* New York: Praeger, 1964.

Giles, Jim. Internet Encyclopedias Go Head to Head. *Nature,* Vol. 438 (December 15, 2005): pp. 900–901.

Gompert, David C. *Heads We Win—The Cognitive Side of Counterinsurgency (COIN): RAND Counterinsurgency Study—Paper 1.* Santa Monica, Calif.: RAND Corporation, OP-168-OSD, 2007. As of June 11, 2007: http://www.rand.org/pubs/occasional_papers/OP168/

Gompert, David C., Irving Lachow, and Justin Perkins. *Battle-Wise: Gaining Advantage in Networked Warfare.* Washington, D.C.: Center for Technology and National Security Policy, National Defense University, January 2005.

Gordon, Michael, Wary Iraqis Are Recruited as Policemen. *New York Times* (July 24, 2006): p. A1.

Headquarters, Department of the Army (and Headquarters, Marine Corps Combat Development Command, Department of the Navy, Headquarters, United

States Marine Corps). *Counterinsurgency.* Washington, D.C.: Headquarters, Department of the Army, Field Manual No. 3-24 (and Headquarters, Marine Corps Combat Development Command, Department of the Navy, Headquarters, United States Marine Corps, Marine Corps Warfighting Publication No. 3-33.5), December 2006.

Huber, Peter. *Orwell's Revenge.* New York: Free Press, 1994.

Joint Chiefs of Staff. *Net-Centric Operational Environment: Joint Integrating Concept, Version 1.0.* Washington, D.C.: U.S. Department of Defense, October 31, 2005. As of June 11, 2007:
http://www.dod.mil/cio-nii/docs/netcentric_jic.pdf.

Kaplan, Jeremy. *A New Conceptual Framework for Net-Centric, Enterprise-Wide, System-of-Systems Engineering.* Washington, D.C.: Center for Technology and National Security Policy, National Defense University, Defense & Technology Paper No. 30, July 2006.

Kramer, Franklin D.. Larry Wentz, and Stuart Starr. *I-Power: The Information Revolution and Stability Operations.* Washington, D.C.: Center for Technology and National Security Policy, National Defense University, Defense Horizons Paper No. 55, February 2007.

Maghan, Jess, Gregory O'Reilly, and Phillip Chong Ho Shon. Technology, Policing, and Implications of In-Car Videos. *Police Quarterly*, Vol. 5, No. 1 (March 2002): pp. 25–42.

"A Micropayment for Your Thoughts," *Wired,* December 1, 2003.

Rosenau, William. *Subversion and Insurgency: RAND Counterinsurgency Study—Paper 2.* Santa Monica, Calif.: RAND Corporation, OP-172-OSD, 2007. As of June 11, 2007:
http://www.rand.org/pubs/occasional_papers/OP172/

Simon, Paul T. "Unit Immersion in Mosul," *Military Review,* July–August 2006.

Smith, Edward. *Effects Based Operations*. Washington, D.C.: Command and Control Research Program (CCRP), Office of the Assistant Secretary of Defense, 2002.

Smith, Rupert. *The Utility of Force.* New York: Knopf, 2007.

Stanton, Major Paul T. Unit Immersion in Mosul: Establishing Stability in Transition. *Military Review* (July–August 2006): pp. 60–70. As of June 11, 2007:
http://usacac.army.mil/CAC/milreview/English/JulAug06/Stanton.pdf

Talbot, David. How Tech Failed in Iraq. *Technology Review* (November 2004): pp. 36–45.

Thompson, Bill. Not as Wiki as It Used to Be. *BBC News* (August 25, 2006). As of June 11, 2007:
http://news.bbc.co.uk/go/em/fr/-/2/hi/technology/5286458.stm

U.S. Department of Defense. *Network-Centric Operations.* Web site, n.d. As of June 11, 2007:
http://www.oft.osd.mil/initiatives/ncw/ncw.cfm

———. *Management of DoD Information Resources and Information Technology.* Washington, D.C.: U.S. Department of Defense, DoD Directive 8000.1, February 27, 2002. As of June 11, 2007:
http://www.dtic.mil/whs/directives/corres/pdf/800001p.pdf

———. *Data Sharing in a Net-Centric Department of Defense.* Washington, D.C.: U.S. Department of Defense, DoD Directive 8320.2, December 2, 2004. As of June 11, 2007:
http://www.dtic.mil/whs/directives/corres/pdf/832002p.pdf

———, Office of Force Transformation. *The Implementation of Network-Centric Warfare,* Washington, D.C.: U.S. Government Printing Office, January 5, 2005a.

———. *Net-Centric Environment: Joint Functional Concept, Version 1.0.* Washington, D.C.: U.S. Government Printing Office, April 7, 2005b. As of June 11, 2007:
http://www.dtic.mil/futurejointwarfare/concepts/netcentric_jfc.pdf

U.S. Marine Corps. *The Small Wars Manual.* Washington, D.C.: U.S. Government Printing Office, 1940.