United States Marine Corps
School of Advanced Warfighting
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

FUTURE WAR PAPER

IDENTIFYING THE INSURGENT

**SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF OPERATIONAL STUDIES**

AUTHOR: Lieutenant Colonel Michael J. Targos, USMC

AY 2007-08

Mentor: Dr. Wray Johnson

Approved: _____

Date: _____

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2008		**00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Identifying the Insurgent	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **United States Marine Corps,School of Advanced Warfighting, Marine Corps University,2076 South Street, Marine Corps Combat Development Command,Quantico,VA,22134-5068**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**27**	

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT

Executive Summary

Title: Identifying the Insurgent

Author: Lieutenant Colonel Michael J. Targos, United States Marine Corps

Thesis: The insurgents' ability to hide among the population is a major aspect of their operations and a challenge for most counterinsurgent forces. However, if the insurgents could be identified from among the population, they would lose their advantage.

Discussion: This paper analyzes the impact of a future technology on counterinsurgency (COIN) operations. The technology presupposes the ability of air and ground platforms to identify positively identify individuals from a distance. Whereas current unmanned aerial vehicles (UAVs) and ground observation devices can "see" people from a distance, these platforms cannot automatically recognize these people from previous observation beyond the degree of accuracy which an observer may provide. When this new capability is employed in a COIN environment, and then networked and its data analyzed, counterinsurgents can gain a decisive advantage over their adversaries.

Recommendation: That research be continued in pursuing observation platforms that can recognize people as individuals. Fielding this technology will not be an all-encompassing solution; however, it directly supports the type of warfare our nation can expect to experience against irregular threats well into the future.

Table of Contents

List of Figures

Introduction

The United States must regain the initiative in conducting counterinsurgency (COIN) operations. Future wars will continue to involve operations against irregular threats like those seen in Iraq and Afghanistan.[1] The ability of insurgents to hide among the population negates almost all conventional military advantages of the counterinsurgent.[2] This has been the case in the majority of counterinsurgencies, the only solution being an efficient intelligence system.[3] The insurgents' ability to "hide in plain sight" is a major aspect of their operations and a challenge for most counterinsurgent forces.[4] However, if the insurgents could be identified from among the population, they would lose their advantage.

Identifying the insurgent shifts the initiative back to the counterinsurgent. Combatants seek to gain and maintain the initiative in order to impose their will on their opponent.[5] Exploiting the counterinsurgent's requirement to protect the entire population, the insurgent remains free to carefully choose his attacks. The counterinsurgent is therefore usually reactive.[6] The counterinsurgent fights by accepted rules of land warfare. Infractions undermine his legitimacy in the eyes of the population.[7] The insurgent, conversely, fights by no such rules. This situation results in restricted freedom of action for the counterinsurgent. Possessing both the initiative and freedom of action, insurgents have a decisive advantage over materially stronger opponents.

This paper examines a realistic future capability to combat insurgencies, achievable in the next 15 years, one that greatly increases the ability to identify insurgents. After defining the capability, the requirement, characteristics, tactical employment, technological precedents, future requirements, impact on insurgent

operations, and likely countermeasures will be analyzed. The need to maintain physical contact requires the counterinsurgent to operate among the population; thus, this paper is presented from the tactical level. Much of current research and development (R&D) focuses on systems designed to defeat conventional adversaries. This requirement exists. However, we are at war today and will continue to face challenges in confronting irregular threats for which we are ill-prepared.

Capability

The capability is defined as an air-ground-based system capable of conducting persistent surveillance over areas of up to 100 square miles for an indefinite period of time, that recognizes people as individuals from altitudes of up to 20,000 feet or ground distances of up to 300 yards, that stores and networks the data performing automated analysis, and retains the ability to integrate manual analysis and search parameters.[8] The aerial element would resemble a squadron of unmanned aerial vehicles (UAVs) equipped with highly-sensitive cameras. The ground-based element would resemble a large pair of binoculars carried by security forces. Both elements are networked by wireless digital communications to operations centers capable of displaying and storing video feeds as well as manually inputted data. The brain of the system is a highly-capable computer that organizes the data. All data is networked and accessible in combat operations centers and portable ground units as depicted in figure 1.

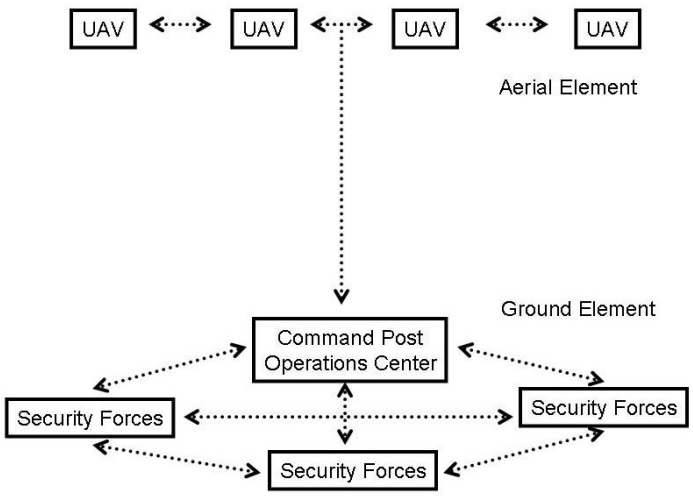

Figure 1 – Depiction of Air-Ground Network

Requirement

Counterinsurgents seek to secure a population by preventing attacks against it. This includes overt physical violence as well as intimidation, subversion, and terrorism.[9] Although insurgency is a political struggle, adaptation and progress in this sphere is impossible without a manageable security situation. Although insurgent activity is typically conducted by relatively small numbers in early stages, its effectiveness and potential are magnified as insurgents remain hidden among the population. The perception is that they are more powerful and capable, and perception is what matters in COIN.[10] But when this small number of insurgents is unable to hide, their small numbers become vulnerable. The population begins to recognize weakness, and the insurgent no longer appears "omni-present." The conditions are set for increasing the public's level of confidence in the counterinsurgent.

Characteristics

The first characteristic of the new capability is *persistent surveillance,* defined as the ongoing systematic observation of aerospace, surface or subsurface areas, places, persons, or things, by visual, aural, electronic, photographic, or other means.[11] Current airborne surveillance systems such as the UAV RQ-1 Predator can "see" individuals from an operating altitude of 25,000 feet, but cannot recognize their identity beyond the degree of certainty which an operator provides.[12] Future persistent surveillance systems will be able to distinguish individuals from similar distances and recognize them if previously observed. For example, if a UAV observes "Ahmed" in Fallujah on a particular date and time, another UAV will be able to recognize the same "Ahmed" when he is observed in Ramadi at a later date. Individual resolution is the key to the capability. Once observed, individuals are assigned a code that can be recalled at a later date.

Once individuals can be recognized from a distance, the need to physically detain and question *suspicious* individuals is minimized. Consequently, wrongful detentions, arrests, and engagements that frustrate the population and weaken the counterinsurgent's cause are also minimized. This is important because insurgents operate among the population and use innocent people as shields or decoys. They provoke overreaction on the part of the security forces and publicize these incidents in order to discredit the counterinsurgent in the eyes of the population.[13]

The second characteristic is the ability to *record* individuals' movements, *store* this information and *access* the information from multiple locations as needed. This creates a detailed chronology of peoples' activities as they relate to situations on the ground. Counterinsurgent forces draw on this archived data to piece together an

intelligence picture or support current operations. For example, if an improvised explosive device (IED) explodes on a street corner that is being watched by a UAV, the counterinsurgent force plays back the recorded data to see who was at that location prior to the explosion. At this point, the capability to distinguish individuals becomes very useful. If someone's identity has already been recorded, that person can be linked to the act of emplacing the IED. Recorded data resembles a movie taken by a video camera with identifications available for the people shown. Analysts or operations personnel move a computer mouse arrow over a person and click to display information pertinent to that individual.

All data is stored and organized by a computer which allows an operator to access an individual's activity. Operators access people or locations as needed when developing an intelligence picture. The information is accessible from various locations. UAVs and operations centers are networked to allow operators with different interests to analyze data. For example, a brigade intelligence officer can use the database to map an insurgent logistics network, while a rifle company commander can use it to confirm a suspicious individual's location that is the target of a search mission. This resembles a combination of laptop computers and handheld devices each of which is capable of displaying the locations of individuals and associated data. This architecture allows operations centers to cooperate with ground units.

The third characteristic is *analysis*. Populated with interactive video, the system also distinguishes trends. In areas where there are frequent hostile acts, for example, those people moving into or out of an area during the same timeframe of the action are automatically identified and brought to the attention of the operator. Operators are able

to zoom in on areas and query who has traveled through the area, recently or in the past. A list of suspicious people is produced. The operator selects individuals and queries their current locations. Since the UAVs conduct persistent surveillance, these people will eventually be found if they remain in the area. At this point, a commander decides whether to continue observing or conduct operations based on the information.

Automated analysis supports human analysis. Human analysis will never be entirely replaced. However, the system will have the capability to answer basic questions for the commander such as "who was at a location at a particular place and time?" Additionally, an operator will be able to construct alerts that are triggered by established criteria. Examples include people traveling to hostile areas, known insurgents moving through peaceful neighborhoods, or previously identified high-value targets (HVTs) seen anywhere in the area of operations. Human operators continuously refine the data as necessary to complete the intelligence picture.

Fictional Architecture Example

With the requirement and characteristics identified, we can construct a scenario to illustrate the concept.

A squadron of UAVs is assigned the mission of identifying the insurgents in a city. There are 24 UAVs in the squadron which are networked to each other and into an archive by wireless digital communications. The archive is located at a unit headquarters along with operations, intelligence, and system maintenance personnel. Complementing the UAVs are 24 ground observation units employed by security forces. The ground units are also networked to the archive. The purpose of the ground units is to complement the aerial observation capability and confirm the identity and location of

individuals during ground operations, such as a patrol, raid, or observation post. All inputs are displayed on screens in an operations center and stored in the archive. A computer constantly screens current inputs and cross references them against the archive looking for identified suspicious individuals or trends that relate to suspicious locations.

Operations center personnel observe the display screens and monitor the alerts given by the computer. Operators adjust the sensitivity of the automatic analysis and focus the aerial observation platforms to complement ground operations. Analysts build an intelligence picture based on the known movements of individuals and compile lists of suspicious personnel. Ground units are notified of suspicious activity. Operations officers direct ground units. Ground units feed back information proving or disproving the analysis.

Technological Precedents and Future Requirements

Given the above scenario, the base capability needed is the ability to recognize individuals from a distance. At present, there are several technologies that a future system might be derived from. The Biometric Automated Toolset System (BATS) has been employed in Iraq and Afghanistan since 2004.[14] Biometrics are physical and behavioral characteristics that identify an individual, such as fingerprints, iris recognition, hand measurements, voice, and gait.[15] Fingerprints, iris scanning, facial recognition, and associated identification cards are in use today. Ideally, multiple biometrics can be observed from a distance in this capability.

Once an individual is identified, he or she is added to a database. This is also in practice today. The future database “catalogs” individuals according to location and activity as shown in figure 2.

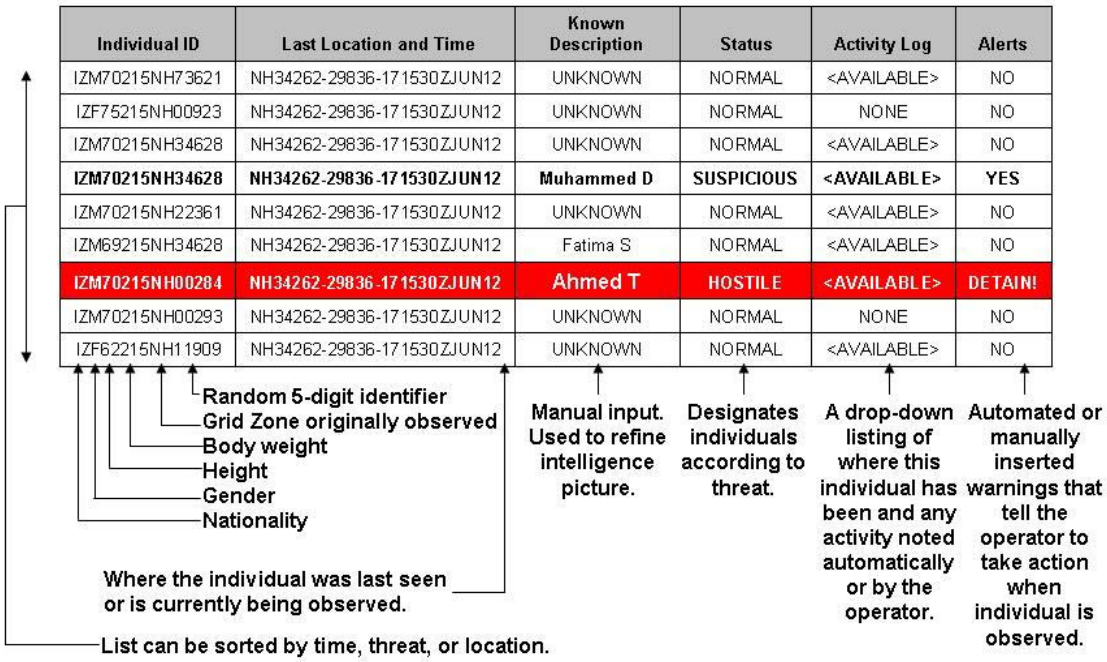

Figure 2 – Sample Catalog Listing of Individuals

The database is built from a combination of auto-population and manual data entry. It is important to retain a manual data entry capability so as to not become totally reliant on the technology. The data is displayed on screens for operators to work off as shown in figure 3.

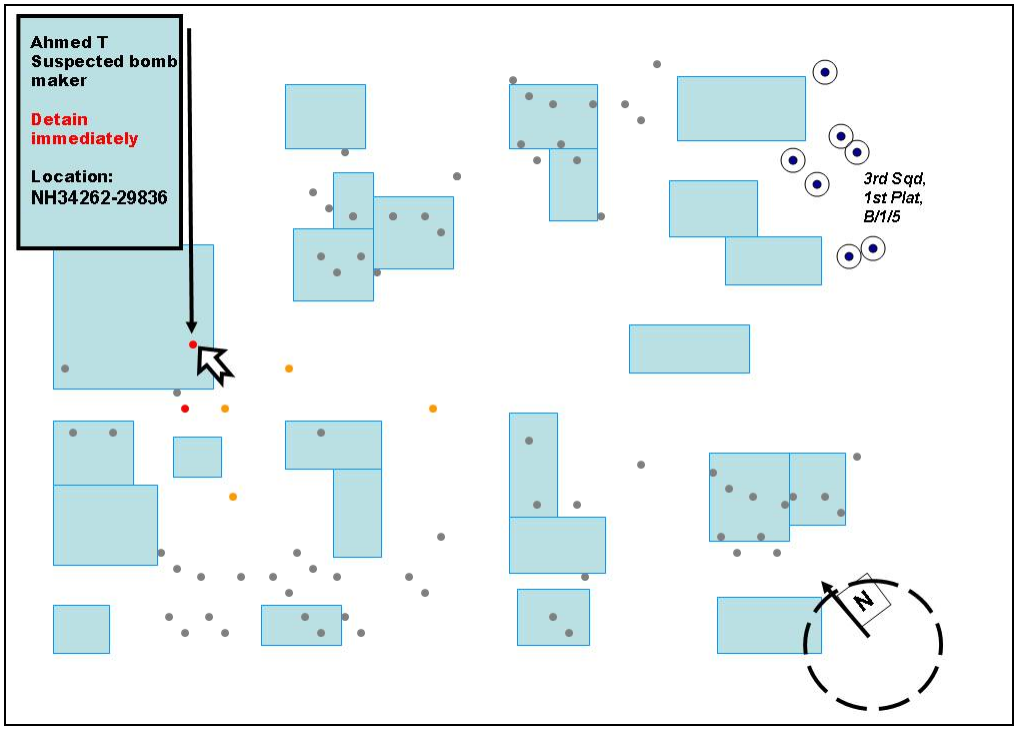

Figure 3 – Sample Display of Threat Information

A ground unit displays smaller, more basic forms of the information geared toward identification of individuals when compared to the UAV as a collection platform.

Tactical Employment

There are four types of employment of this capability in counterinsurgency operations.

1) *Area*. This is the most common type of employment. When employed in this manner, an area affected by insurgency is continually observed by platforms. The movement of people is recorded and analyzed. The area is selected based on its priority in the campaign plan. For example, in Iraq the city of Ramadi is significant as a provincial capital making it a prime candidate for observation. Counterinsurgent forces plan and execute operations based on data collected within the observed area. The

desired effect is to pacify an important area, initiate infrastructural and political reforms, and move the capability to another area within the context of the campaign plan.

2) *Point*. Border crossing sites are an example of point surveillance. When employed in this manner, platforms are focused on a smaller area, perhaps one square mile, where human and vehicle traffic is restricted. Point surveillance is more appropriate for temporary missions or operations designed to interdict insurgent movements. For example, if a shipment of munitions is expected through a certain point, platforms can move and focus for a short period of time in order to identify targets in support of checkpoint operations.

3) *Long Range Individual*. This method of surveillance is used when following someone who is suspected of playing a major role in an insurgency. Explosives experts and insurgent cell leaders are examples. Employing this method, one person is observed and his activities are cataloged, building a larger intelligence picture of an insurgent network. This method of employment is useful to map an insurgent network.

4) *Expeditionary*. In the expeditionary role, a squadron of UAVs is deployed to conduct cross-border operations with the consent of a host nation government during the early stages of a suspected insurgency. The most preferable time to engage an insurgency is in its infancy, when it is most vulnerable.[16] The problem for the counterinsurgent force is that the signs of an insurgency are often unintelligible during this period; thus, the decision to actively oppose a movement is difficult. Once an insurgency is recognized, there is usually a network established to facilitate operations against the government and its counterinsurgent force.[17]

Impact on Insurgent Operations

A typical insurgent operation is the ambush. An ambush consists of a movement to the ambush site, selection of a kill zone, establishing an ambush position, engagement of a target, and a rapid withdrawal.[18] During any of these stages an insurgent may be vulnerable to aerial or ground observation. Typical methods of concealment are to use darkness, vegetation, and urban structures. It is rare, however, that every stage of an ambush operation is perfectly concealed. The ambusher is particularly vulnerable during withdrawal.[19] It is at this point that the counterinsurgent can seize the initiative by recording who participated in the ambush and their movements. The end result is compromise of the insurgent who participated in the hostile act. Cataloged and recorded, those who take part in an ambush are linked to insurgent activity and detained with increased certainty as directed by the commander.

Sniping is another common insurgent operation. Effective sniping shares many of the same movement requirements as an ambush, although snipers typically operate in smaller numbers.[20] Counter-sniper operations require more time to conduct. During a sniper attack, security forces attempt to record the sniper from ground observation units to complement UAV coverage. Since snipers usually practice stealth in exiting a position, the surrounding area is watched for individuals leaving the area. Ground forces then conduct a cordon and search of the area. All structures and concealed areas are searched and the inhabitants brought outdoors where UAVs can observe them. Simultaneously, the computer cross-references peoples' locations against known residences and situations from previous sniper attacks.

If the sniper is able to escape before the cordon is set, UAVs would likely record the movement. Movement through structures or dense vegetation is slow and requires extensive preparation from an insurgent security force or supportive civilian population. To expedite departure from the area, a sniper would likely hide his weapon and attempt to blend with the population. At this point he is vulnerable to observation by ground and aerial assets.

Simple IEDs are rapidly emplaced. To be an effective casualty-producing weapon, however, they require a trigger man who can observe the kill zone, camouflage the device, and prepare the ground.[21] These three requirements make the perpetrator vulnerable to observation and recording. Whether exposing himself to aerial observation while emplacing the IED or remaining in the vicinity to detonate the device, the insurgent can be identified. As shown in Figure 4, the network required to employ IEDs in support of an insurgency is extensive and consists of many nodes. Each of these relationships has vulnerabilities that can be exploited by the capability.

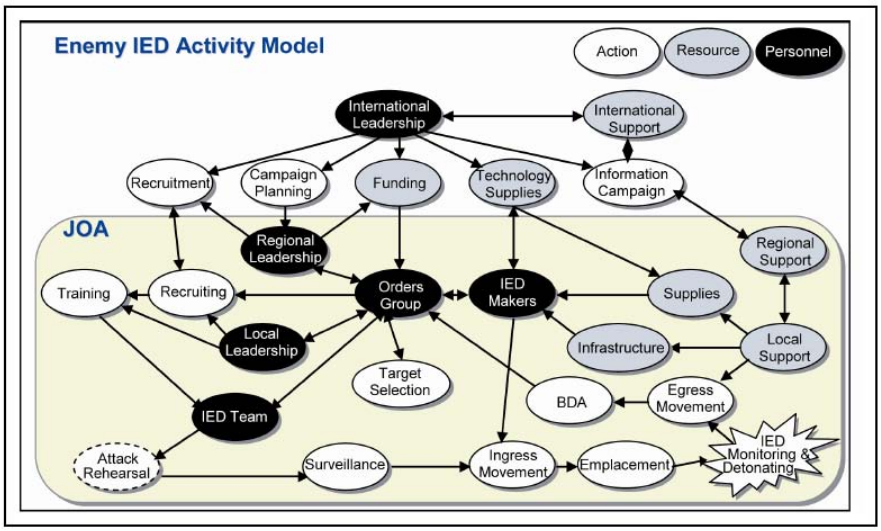

Figure 4 - Source: Field Manual Interim 3-34.119/Marine Corps Information Publication 3-17.01. *IED Defeat*

Particularly in the early stages of an insurgency, insurgents need access to the population for support and to intimidate key individuals. The capability described in this paper can be used to populate a census. Should an insurgent movement send individuals to an area they intend to control, the capability would detect the intrusion. Additionally, it can help determine what areas or particular public figures are the targets of intimidation. At this point, counterinsurgent security forces can detain suspected insurgents and provide additional security to targeted areas. Surprise employment of the capability is suited to counter this type of insurgent operation. Ideally, insurgents do not know the area is under surveillance. They move overtly while information is collected on them, and an operation is planned to reverse the effects of intimidation.

Insurgencies typically operate on a fragile logistical foundation unless matured and redundant.[22] The logistical system of an insurgent movement must operate in near perfect secrecy if fighting against this capability. One observed attack, an IED for example, could be traced all the way back to the origin of the explosives exposing the insurgent, the transporter of the device and components, and the supplier.

Insurgencies need to recruit members in order to grow. Identification operations[23] focus on discrediting the insurgent recruitment effort by tracking and disrupting new members. For example, the analysts could watch as someone assessed to be an insurgent recruiter gather prospective insurgents. At this point, security forces can intervene and notify the new member that he is being watched, or detain the recruiter.

Counterinsurgents quickly gain momentum in information operations with the capability. Suspected members of an insurgent movement can be confronted by security forces before or after hostile acts are performed. Notifying selected individuals of their

discovered affiliation with the insurgency would have powerful psychological effects. Suspicion in the ranks of an insurgency is the worst possible situation for that organization. Covert organizations require high levels of trust to remain hidden from counterinsurgents. Without that trust, operations break down. British operations in Malaya from 1950-1952 exemplify successful exploitation of insurgent suspicion within their organization.

Historical Example: The Malayan Emergency

Prior to 1951, British counterinsurgency efforts were plagued by a lack of actionable intelligence regarding the Malayan Communist Party (MCP).[24] Several initiatives failed to stabilize the security situation. Hampered by organizational problems and a Chinese squatter population that supported the communist insurgency, the British eventually turned the tide of the insurgency by emphasizing police intelligence over combat operations.[25]

Realizing that efficiently conducted security operations would seriously affect MCP morale and cohesion, Sir Gerald Templar instituted organizational, personnel, and tactical changes. From a more efficient intelligence organization, all success would flow. Exploiting the communist insurgency's inherently suspicious nature, he executed Operation LETTER BOX, which solicited anonymous information on insurgent operations from the Chinese squatter population.[26] From these separate pieces of information, a campaign was begun to bring MCP personnel and insurgent-supporting squatters to the side of the Malayan government.

Templar's efforts were psychological in nature, with tactical actions carefully designed to create suspicion in the MCP and its supporters.[27] By soliciting the

information anonymously, coercion, at least temporarily, ceased to be an effective insurgent tactic. Moreover, insurgents began to worry about betrayal. The MCP relied on sustenance from the squatters, but when the link-ups were ambushed between them and their supporters, both parties became overly cautious. The net result was less food for the insurgents.[28]

The British in Malaya had employed an identification card system from the earliest days of the emergency, but it was poorly enforced. The MCP made squatters tear up their cards, and the lack of security force presence could not prevent their destruction.[29] When a stronger effort was made to enforce the identification card system with more and better trained police, the results were immediate. Counterinsurgent security forces could monitor movement between villages and detain personnel in areas in which they did not reside. The effect on the insurgency was slower, less responsive communications and less communist presence in the squatters' villages.[30] Counterinsurgent tempo increased.

A complementary program focused on exploiting surrendered enemy personnel (SEP) and integrating them into COIN operations.[31] In perhaps the most imaginative use of available assets, transport planes fitted with loudspeakers flew over the jungle broadcasting insurgent names and personal information for MCP members to hear. The voices on the broadcasts were often former insurgents appealing to their comrades in the jungle to surrender.[32] Combined with radio broadcasts, security operations, and well-organized resettlement, these appeals to the MCP weakened the organization to the point where British and Malayan government momentum became irreversible.

The improved surveillance capability described in this paper could be used to achieve similar effects resulting in the confidence of the population and suspicion within the insurgent movement. Police work would be enhanced. An identification card system would be verified. Combat operations would be planned to minimize collateral damage against civilians. Detained insurgents would be interrogated based on detailed evidence of their activity and contacts. In the end, an insurgency would need to operate in such secrecy that its influence on the population could be countered.

Insurgent Countermeasures

The natural reaction to a capability such as observation from a distance is to stay concealed inside structures or vegetation, or descend below the surface into tunnels or sewers. There are two counters to such insurgent countermeasures. One is the systematic searching of areas that force people into the open for observation. This has no effect on the population other than standing outside while a UAV or ground unit observes them. To insurgents, it is the equivalent of a source pointing a finger at them and identifying them as insurgents.

The second way to combat concealment is to be able to see through structures, vegetation, or the ground. It is conceivable that a future UAV carrying improved observation technology could see through these obstructions. Ground-penetrating radar is a current technology that can see through structures and earth. It is used in law enforcement and archeology.[33] Advanced application of this capability would seek a higher resolution so as to be able to distinguish individuals indoors, in vegetation, or underground. This additional capability would further reduce the insurgents' ability to

hide. At that point, it is difficult to imagine a countermeasure that would conceal an insurgent's identity over a prolonged period of time.

If insurgents can be identified and cataloged, making them vulnerable, another counter to the capability would be to use people for a one-time strike on counterinsurgent forces. Suicide bombers coming across a border or an otherwise would-be civilian who is willing to attack counterinsurgents for money are difficult to stop. In both cases, if a group of insurgents cannot operate against counterinsurgent forces on an enduring basis, the insurgent organization is denied veteran combatants and is thus less effective. Suicide bombers also need a great deal of coordination to be effective. They need transportation, guiding, and planning to support their attack. These three aspects of a suicide attack would need to come from a member of an insurgent organization who could be targeted by the capability identified in this study.

Conclusion

Technology will never be a stand-alone answer to insurgencies. Identifying the insurgent will always be a requirement, however. The proposed capability outlined in this paper will support human actions. That said, commanders must safeguard against being wholly reliant on technologically-based intelligence collection. Historically, less sophisticated counterinsurgents are most effective by their work among the population.[34] Human intelligence will continue to be the cornerstone of effective counterinsurgency operations. The capability to identify the insurgent will enable counterinsurgents, however, to operate with more precision and with potentially higher success rates. This is critical in demonstrating to the population the counterinsurgent's ability to counter the threat.[35]

Application will take time. The capability will not be foolproof. Nor will it provide instant solutions to the interactively complex problem of insurgency. It is only a tool for the counterinsurgent commander. Nevertheless, with this capability at his disposal, the commander will be free to think before he acts, thus decreasing the amount of wrongful arrests, collateral damage, and undue stress on the population. The need to identify the insurgent is worthy of continued research and development. For the foreseeable future, the United States will be at war with those who would maximize their ability to exploit the law of land warfare. At the very least we should strive to fight them on equal ground.

Notes

1. Joint Publication (JP) 1-02 defines irregular forces as "armed individuals or groups who are not members of the regular armed forces, police, or other internal security forces." Joint Pub 1-02, Operational Terms (Washington D.C.: The Joint Chiefs of Staff, date), 280.

2. David Galula, Counterinsurgency Warfare – Theory and Practice (New York: Praeger, 2005), 6. See also Robert R. Tomes, "Relearning Counterinsurgency Warfare," *Parameters* (Spring 2004): 27.

3. Galula, 72; Tomes,19.

4. Frank G. Hoffman, "Neo-Classical Counterinsurgency?" *Parameters* (Summer 2007): 85.

5. Marine Corps Doctrinal Publication 1, *Warfighting* (Washington D.C., Headquarters U.S. Marine Corps, 1997), 32. Hereafter referred to as MCDP-1.

6. Galula, 11.

7. Galula, 14, 15.

8. These parameters were selected based on the requirement to observe a city approximately the size of Baghdad (approximately 80 square miles) and a conservative estimate of effective small arms range in an urban environment (300m).

9. Galula, 27-33.

10. Field Manual 3-24/Marine Corps Warfighting Publication 3-33.5, *Counterinsurgency* (Washington D.C.: Department of the Army, December 2006), 1-113. Hereafter referred to as FM 3-24.

11. JP 1-02 defines *surveillance* as "the systematic observation of aerospace, surface or subsurface areas, places, persons, or things, by visual, aural, electronic, photographic, or other means." *Persistent surveillance* only adds the word "ongoing" to the beginning of the definition because observation duration is indefinite. JP1-02, 525.

12. MAGTF Staff Training Program Pamphlet 5-0.3, *MEF Planner's Reference Manual*, 2006, 42. The UAV data section of this manual was updated April 2006. The RQ-1 Predator was selected as a template for the capability because of its ability to operate for a long duration of 40+ hours and its capability to support tactical units or national level commands.

13. FM 3-24, 1-152, A-25. See also Steven Metz, *Learning From Iraq*: *Counterinsurgency in American Strategy* (Carlisle, Pa.: US Army War College, Strategic Studies Institute, January 2007), 28-30.

14. Lionel Beehner, "Backgrounder: A National ID Program for Iraq?" *The New York Times*, 29 May 2007. Available at http://www.nytimes.com/cfr/world/slot2_ 20070529.html.

15. Donna Miles, "Biometrics Helping Identify Foes in War on Terror," *American Forces Press Service News Articles, American Force Press Service*, Washington D.C., 5 November 2004. Available at http://www.globalsecurity.org/security/library/news/2004/ 11/sec-041105-afps01.htm.

16. Galula, 26.

17. Galula, 4,5.

18. Marine Corps Warfighting Publication 3-11.3, *Scouting and Patrolling*, (Washington D.C.: Headquarters, U.S. Marine Corps, 2000), 13-4 to 13-7.

19. Ali Ahmad Jalali and Lester W. Grau, The Other Side of the Mountain: Mujahadeen Tactics in the Soviet-Afghan War (Quantico, Va: The United States Marine Corps Studies and Analysis Division, 1998), 373-390. Chapter 14 examines urban combat. Repeatedly, the Mujahadeen spoke of the importance of securing their approach and withdrawal through urban areas. At times, up to 80% of an ambush force was dedicated to security of the route of withdrawal.

20. Marine Corps Warfighting Publication 3-15.3. *Sniping*, (Washington D.C.: Headquarters, U.S. Marine Corps, 2004), 1-4, 1-5, 4-16, 4-17, 4-29, and 4-30.

21. Field Manual Interim 3-34.119/Marine Corps Information Publication 3-17.01. *IED Defeat* (Washington D.C.: Department of the Army, Headquarters U.S. Marine Corps, September, 2005), 3-1 to 3-3.

22. Galula 25, 26.

23. The author of this paper defines identification operations as operations undertaken to establish known identities for a population or portion thereof. There is no joint definition in JP 1-02.

24. Kumar Ramakrishna, Emergency Propaganda: The Winning of Malayan Hearts and Minds, 1948-1958 (Richmond, Surrey: Curzon Press, 2002), 204.

25. Richard Clutterbuck, The Long, Long War: The Emergency in Malaya, 1948-1960 (Singapore: Cultured Lotus, 2003), 85.

26. Ramakrishna, 140.

27. Ramakrishna, 140.

28. Ramakrishna, 141,142.

29. Clutterbuck, 68.

30. Clutterbuck, 89.

31. Ramakrishna, 153, 154.

32. Ramakrishna, 154, 155.

33. Ground penetrating radar. "It is used in archaeology and law enforcement for locating clandestine graves and buried evidence. Military uses include detection of mines, unexploded ordnance, and tunnels." See: http://www.archaeophysics.com for more information.

34. Galula, 32.

35. Tomes, 27.

Bibliography

Archaeo-Physics, Shallow Subsurface Geophysical Survey. "Ground Penetrating Radar." <http://www.archaeophysics.com> (2008).

Beehner, Lionel. "Backgrounder: A National ID Program for Iraq?" The New York Times, 29 May 2007. Available at http://www.nytimes.com/cfr/world/slot2_ 20070529.html.

Clutterbuck, Richard. The Long, Long War: The Emergency in Malaya, 1948-1960. Singapore: Cultured Lotus, 2003.

Department of the Army, Field Manual 3-24/Marine Corps Warfighting Publication 3-33.5: Counterinsurgency. Washington D.C. December 2006.

Department of the Army, Field Manual Interim 3-34.119/Marine Corps Information Publication 3-17.01: IED Defeat. 2005.

Galula, David. Counterinsurgency Warfare – Theory and Practice. New York: Praeger, 2005.

Hoffman, Frank G. "Neo-Classical Counterinsurgency?" Parameters, 37, no. 2 (Summer 2007): 71-87.

Jalali, Ali Ahmad and Grau, Lester W. The Other Side of the Mountain: Mujahadeen Tactics in the Soviet-Afghan War. Quantico, VA.: The United States Marine Corps Studies and Analysis Division, 1998.

Metz, Steven. "Learning From Iraq: Counterinsurgency in American Strategy." Carlisle, Pa.: Strategic Studies Institute, U.S. Army War College, January 2007.

Miles, Donna. "Biometrics Helping Identify Foes in War on Terror," American Forces Press Service News Articles, American Force Press Service, Washington D.C., 5 November 2004.

Ramakrishna, Kumar. Emergency Propaganda: The Winning of Malayan Hearts and Minds, 1948-1958. Richmond, Surrey: Curzon Press, 2002.

The Joint Chiefs of Staff, Joint Publication 1-02: Operational Terms. Washington D.C.: March 2008.

Tomes, Robert R. "Relearning Counterinsurgency Warfare." Parameters 34, no. 4 (Spring 2004): 16-28.

United States Marine Corps, MAGTF Staff Training Program Pamphlet 5-0.3: MEF Planner's Reference Manual. Quantico, Va.: 2006.

United States Marine Corps, Marine Corps Warfighting Publication 3-11.3: Scouting and Patrolling. Washington D.C.: 2000.

United States Marine Corps, Marine Corps Warfighting Publication 3-15.3: Sniping. Washington D.C.: 2004.

United States Marine Corps, Marine Corps Doctrinal Publication 1: Warfighting. Washington D.C.: 1997.