Calhoun
Institutional Archive of the Naval Postgraduate School

Author(s)	Clark, Joel J.
Title	The effects of information technologies on insurgency conflict : framing future analysis
Publisher	Monterey, California. Naval Postgraduate School
Issue Date	1998-12
URL	http://hdl.handle.net/10945/32616

This document was downloaded on March 14, 2014 at 05:55:17

DUDLEY KNOX LIBRARY

Calhoun is a project of the Dudley Knox Library at NPS, furthering the precepts and goals of open government and government transparency. All information contained herein has been approved for release by the NPS Public Affairs Officer.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

http://www.nps.edu/library

http://www.nps.edu/

NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

THE EFFECTS OF INFORMATION TECHNOLOGIES ON INSURGENCY CONFLICT: FRAMING FUTURE ANALYSIS

by
Joel J. Clark

December 1998

Thesis Advisors: Gordon McCormick
Erik Jansen

DTIC QUALITY INSPECTED 4

Approved for public release; distribution is unlimited.

19990219028

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE December 1998	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE
THE EFFECTS OF INFORMATION TECHNOLOGIES ON INSURGENCY CONFLICT: FRAMING FUTURE ANALYSIS

5. FUNDING NUMBERS

6. AUTHOR(S)
Clark, Joel J.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES
The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

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

12b. DISTRIBUTION CODE

13. ABSTRACT *(maximum 200 words)*

The purpose of this thesis is to develop a framework to analyze the impacts of information technologies on future insurgency conflict. This objective is achieved by analyzing an existing communications model for internal war and identifying factors that will affect the use of information technology by either belligerent. These factors impact the ability of either the state government or insurgent organization to influence the state's population and international community in the struggle for state power. The factors identified range from the internal conductivity of a society to the type of government that exists within a state. Identified factors are then incorporated into the communications framework to act as a model to identify strengths and weaknesses within any specific campaign.

This thesis also addresses the interactive nature of insurgency conflict. Depending upon the information technology capability of a government or insurgent force, in which scenarios is it more beneficial to incorporate an offensive and in which a defensive strategy, given the capabilities of an opponent? This thesis is designed to be a starting point for future analysis of how emerging information technologies impact the struggle for state power between an existing government and a rebel organization within its borders.

14. SUBJECT TERMS
Insurgencies, Information Technologies, Internal Conflict, Guerrilla War

15. NUMBER OF PAGES
63

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFI- CATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev..2-89)
Prescribed by ANSI Std. 239-18

Approved for public release; distribution is unlimited

THE EFFECTS OF INFORMATION TECHNOLOGIES ON INSURGENCY CONFLICT: FRAMING FUTURE ANALYSIS

Joel J. Clark
Major, United States Army
B.B.A., University of Iowa, 1987

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN DEFENSE ANALYSIS

from the

NAVAL POSTGRADUATE SCHOOL
December 1998

Author: [redacted]

Joel J. Clark

Approved by: [redacted]

Gordon McCormick, Thesis Advisor

[redacted]

Erik Jansen, Thesis Advisor

[redacted]

Maurice D. Weir, Chairman
Special Operations Curriculum
Committee

ABSTRACT

The purpose of this thesis is to develop a framework to analyze the impacts of information technologies on future insurgency conflict. This objective is achieved by analyzing an existing communications model for internal war and identifying factors that will affect the use of information technology by either belligerent. These factors impact the ability of either the state government or insurgent organization to influence the state's population and international community in the struggle for state power. The factors identified range from the internal conductivity of a society to the type of government that exists within a state. Identified factors are then incorporated into the communications framework to act as a model to identify strengths and weaknesses within any specific campaign.

This thesis also addresses the interactive nature of insurgency conflict. Depending upon the information technology capability of a government or an insurgent force, in which scenarios is it more beneficial to incorporate an offensive and in which a defensive strategy, given the capabilities of an opponent? This thesis is designed to be a starting point for future analysis of how emerging information technologies impact the struggle for state power between an existing government and a rebel organization within its borders.

TABLE OF CONTENTS

I. INTRODUCTION.....1

A. INFORMATION TECHNOLOGIES AND MODERN WAR.....1

B. INSURGENT ORGANIZATIONS AND MODERN WAR.....4

C. METHODOLOGY AND APPROACHES.....8

D. A LOOK AHEAD.....9

II. INFLUENTIAL FACTORS IN THE USE OF INFORMATION TECHNOLOGIES.....11

A. INTERNAL INSURGENCY COMMUNICATIONS.....12

B. COMMUNICATING WITH THE STATE'S POPULATION..... 18

C. COMMUNICATING WITH THE INTERNATIONAL COMMUNITY.....25

D. THE STATE GOVERNMENT VERSUS THE INSURGENTS.....33

E. CHAPTER CONCLUSIONS.....38

III. APPLICATIONS TO THE FUTURE.....41

A. THE UNEVEN FUTURE BATTLEFIELD.....41

B. INTERACTIVITY BETWEEN HIGH-LOW TECHNOLOGY.....43

C. CONCLUSIONS.....46

SELECTED BIBLIOGRAPHY.....49

INITIAL DISTRIBUTION LIST.....51

LIST OF FIGURES

1. Figure 1. Information Benefits to the U.S. Military.....3

2. Figure 2. The Communication Needs of an Insurgency.....5

3. Figure 3. Influential Factors in the Use of Information Technologies.....39

4. Figure 4. Interrelationship Between High-Low Tech Opponents.....44

I. INTRODUCTION

Information technologies have transformed nearly every aspect of the world in which we live. Whether the telegraph or the networked computer, tools that enable individuals, organizations, and their decision makers to interact and process greater amounts of information at faster speeds have made an impact on everything from the optimal structure of organizations to the ways in which nations wage war. Just as the corporate world continues to expand its uses of information technologies to transform the business landscape, governments are increasingly turning to these technologies to aid them in combating their adversaries.

Most of the government attention has concentrated on analyzing the effects of information technologies in conventional state-on-state conflicts. Little attention has been given to examining the ways in which technology may affect internal wars. Given a certain level of security, will the introduction of information technologies increase the efficiency of an underground organization? The tension between the added efficiency of technology employment and the general decrease in security is essential to understanding the impact of information technologies on internal conflict. This tension must be examined in both offensive and defensive terms, as well as the point at which the technology's marginal returns outweigh the marginal costs, to determine the extent of the impact that information technologies might have in an insurgency campaign.

A. INFORMATION TECHNOLOGIES AND MODERN WAR

Within most advanced societies, the military has been profoundly touched by developments in communications and other information technologies. The swift and

decisive victory by Coalition Forces in the Iraq desert demonstrated the utilities of a force that held a distinct advantage in information technologies. These changes in the conduct of war have stimulated discussion of a Revolution in Military Affairs (RMA) and have left historians such as Steven Metz and James Kievit comparing today's changes with those brought about by the advent of gunpowder[1]. Whether the change in conduct of military affairs is "revolutionary" or "evolutionary" is beyond the scope of this paper. What is clear, however, is that technological changes have profoundly affected modern military decisionmaking.

The decision cycle depicted in Figure 1 shows the evolution of the process of turning information into action. In this continuous process, information is entered into the cycle, where it becomes intelligence. This intelligence is the basis for planners and decisionmakers to orient themselves to any given situation and determine their course of action. If an opponent can affect the accuracy or impede the information received by an adversary, then he has altered that adversary's decision process. Thus, as advanced systems rely more heavily on information to execute specific tasks and decisions, the systems that transport the given information become an important commodity. Although this process has remained intact throughout history, the speed and intensity with which it functions has changed dramatically.

Figure 1 below also demonstrates how portions of the decision cycle have been profoundly altered by information technologies in the short history of America's military. Advances in technologies have created an environment in which information received is

[1] Metz, Steven and Kievit, James. The Revolution in Military Affairs and Conflict Short of War. Strategic Studies Institute: U.S. Army War College. July 25, 1994.

now acted upon in a matter of minutes, compared to the months in Grant's or Washington's day. The importance of reliable and accurate information has never been greater than it is today. This added reliance on information has placed the decision cycle under stresses never before experienced and has made information and the technologies that transport that information a key ingredient in any military endeavor.

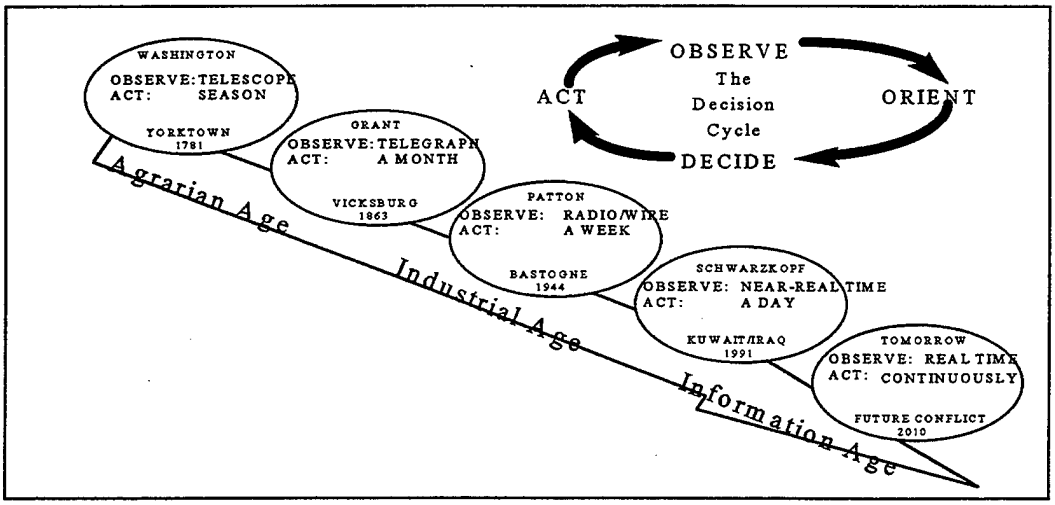

Figure 1. Information Benefits to the U.S. Military[2]

Conflicts waged between states are not the only conflicts to be influenced by the introduction of faster information tools. Internal wars waged between states and insurgents are just as likely to be significantly influenced by developing technologies. Information technologies can provide an important instrument with which an out-gunned,

[2] Adapted from Rose, John BG, American Army Introduction to the 21st Century, given by briefer Martin Hill of Booz Allen & Hamilton Inc., 1998.

out-manned, and generally out-resourced guerrilla force may compete for the power of a state.

B. INSURGENT ORGANIZATIONS AND MODERN WAR

Insurgencies and insurgent movements have been present as long as there have been state governments. Organizations and individuals that hold a disproportionately low or nonexistent level of power have often attempted to seize control of a government and monopolize the resources to the benefit of their constituents. The struggles of Mao, Ho Chi Minh, and Fidel Castro are all well documented and have resulted in the transformation of states from one government to a new political system in a winner-take-all game for state power. Other more limited successes have resulted in numerous spin-offs and fragmentations as various insurgent organizations partake in their respective struggles for power.

Gordon H. McCormick, professor at the Naval Postgraduate School, designed the framework depicted in Figure 2, slightly modified for this purpose, to depict at the macro level the forces at play in an insurgent struggle within a state. The two major adversaries, the state and the insurgents, contend for influence over the state's population and the international community. The solid arrows represent communications channels attempting to influence through a variety of means both the populace and the international community by the insurgents and the existing state. The dashed arrows represent attempts to disrupt that influence. The arrows depicted in the framework assume different characteristics depending upon their respective origins and targets.

The three arrows that extend from the state government on the model represent attempts to influence or control the actions or inaction of the state's population, the

international community, and the insurgent organization. The arrows that lead to the state population and international community are primarily defensive in nature. The government attempts to decrease tolerance for the insurgents within the population.[3] The arrow that aims toward the insurgents is primarily offensive. The state takes aggressive actions to limit the disruption that the insurgents can cause to the state's ability to function legitimately and efficiently. The actions taken usually fall to the military or police apparatus of a state; destruction, force, and arrest are the primary tools employed.

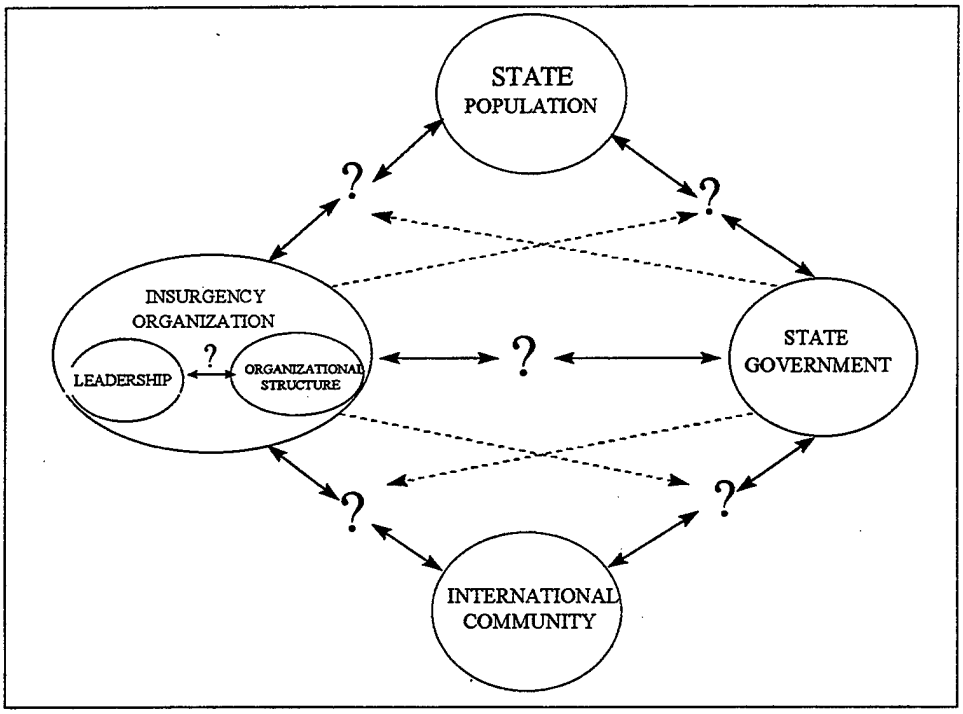

Figure 2. The Communication Needs of an Insurgence[4]

Of the three arrows emanating from the insurgent organization, two are offensive in nature and the other defensive. The insurgents attempt to change the status quo by influencing both the state's population and the international community. These actions,

[3] Leites, Nathan, and Wolf, Charles Jr. Rebellion and Authority: An Analytic Essay on Insurgent Conflicts. (RAND, February 1970).
[4] This model is presented in the "Seminar on Guerrilla Warfare".

usually offensive, can range from image management to open acts of terrorism against the state's population. The arrow that points from the insurgents to the state government is operationally defensive in nature, as is the one describing internal communications. Rebels use covert and secretive techniques to remain anonymous to the standing government, preventing government forces from eliminating them through arrest, expulsion, or death. This secrecy is a major component in the insurgents' ability to remain viable in the face of government forces that out-gun, out-man, and generally out-resource them.

Secrecy is an essential ingredient for the insurgents' success. Direct confrontation is related to the government's ability to identify or "see" the insurgents. Once the guerrilla group can be identified, the government can "hit" it with a variety of weapons, ranging from prison time or expulsion to actual physical destruction of individual guerrillas. This "see-hit"[5] relationship is essential to the understanding of the likelihood of success or failure of an internal war. All things being equal, the more anonymous insurgents can remain, the more likely they are to be successful in their battle to obtain power. The more likely it is that the government can identify the guerrilla, the more likely the government will be able to eliminate the opposition and remain in power. Anonymity, however, is not free. The security of an insurgent group directly affects the efficiency with which it is able to accomplish its mission of replacing the standing government.

J. Bowyer Bell has discussed the inherent inefficiency in the secrecy in which insurgents must conduct their actions. According to Bell, an inverse ratio exists between

[5] Notes, "Seminar on Guerrilla Warfare" at the Naval Postgraduate School.

secrecy and efficiency: absolute secrecy guarantees that nothing works properly.[6] A guerrilla force must communicate to operate. An idea not communicated is worthless to any insurgent cause. Whether communication is among rebels or between the insurgents and the international community, the exchange of information must take place for ideas to spread. However, communicating requires that the rebels expose themselves to forces that oppose them. As insurgents gain strength through the indigenous support of the population or the exogenous support of foreign actors, they increasingly defy and challenge the government in open confrontation. Every rebel who attempts to communicate may provide the essential information that exposes his identity to the state. The underground is inherently more inefficient than a government that does not operate in such an oppressive environment.

Information technologies have generally increased the efficiency with which organizations are able to receive, process, and act upon information. The insurgency model depicted in Figure 2 outlines the communications requirements within any insurgent struggle. These communication requirements seem absurdly simple until the underground organization's security constraints are considered. Will the underground remain as inefficient with the introduction of information tools? What factors will influence the use of information technologies within an internal struggle? Where will the relative advantage lie when marginal costs are compared to marginal returns? In what situations will it be more conducive to employ offensively or defensively oriented information systems within an insurgency or counterinsurgency campaign?

---

[6] Bell, J. Bowyer. "Aspects of the Dragon World: Covert Communications and the Rebel Ecosystem," International Journal of Intelligence and Counterintelligence, Volume 3, Number 1.

C. METHODOLOGY AND APPROACHES

In asking the question, "How will information technologies affect insurgent organizations?", this research develops an existing framework to identify factors relevant to the future uses of information technologies in internal wars. The focus is on the tension generated by the introduction of tools that increase efficiency in an environment that is inherently inefficient due to security concerns. This research uses the previously presented insurgency-counterinsurgency framework to identify the communications requirements of an internal war and to identify those factors that influence an insurgent group's ability to use information technologies to meet these requirements. The analysis then examines where the relative advantages or disadvantages lie with respect to a specific internal war. The relative advantages are examined interactively, the state versus the guerrillas, to determine how relative strengths and weaknesses affect the strategy employed by an opponent.

This research is exploratory. It would be naïve to believe that it will provide the definitive analytic model on the effects of information technologies on internal wars. As the information era brings rapid changes to societies and their war-fighting capabilities, the techniques and tactics of internal war will change just as rapidly. This analysis should be used as a starting point for future research to determine both the possible tactics and countermeasures of specific counterinsurgency campaigns.

D. A LOOK AHEAD

Following this introductory chapter, Chapter II develops the factors that impact the uses of information technologies on an internal conflict. Factors are identified using the insurgency-counterinsurgency framework as the basis of determining the

communications requirements of both the state and the insurgent organization. The factors are intended to develop a starting point for future research into the possible advantages held by both the state and the insurgent organization. They are used to develop the framework and specify determinants of possible relative advantages or disadvantages that may exist with regard to both the insurgents and the state.

Chapter III examines where the relative advantages lies within any insurgency conflict. This chapter looks at both high- and low-technology insurgents and state governments to illuminate under what circumstances the use of information technologies may serve as an advantage or a liability, depending upon the adversary's capability. This chapter also looks at circumstances in which the need for more defensive approaches are necessary. Circumstances in which the relative advantage may lie in the employment of more offensively oriented technologies are also discussed. The offensive-defensive question is addressed by examining where vulnerabilities may lie between capabilities and susceptibilities.

II. INFLUENTIAL FACTORS IN THE USE OF INFORMATION TECHNOLOGIES

This analysis begins with the factors that influence the employment of technology within a society under siege. The McCormick Model (Figure 2) framework of the communications requirements within an insurgency campaign is used to identify the elements that contribute to the potential use of information tools to affect the outcome of a sub-state conflict. A macro level analysis of this nature discounts much of the cultural and societal specifics that significantly affect the everyday working environment of insurgents and their organizations. Designed as an overview of insurgences, this chapter excludes discussions of the societal customs, mores, and beliefs that play a significant part of any analysis of specific insurgences past, present, or in the future.

As critical factors are identified, they will be added to the framework. This list of factors is a starting point in the analysis of any ongoing or potential insurgency campaign; it can be used to determine the capability of technologies to change the outcome of a campaign. The identified factors are not intended to be all-inclusive. As new technologies emerge and the societies they affect develop and mature, further analysis should be conducted to identify any new salient elements. With this restriction, here are the factors that are prevalent in the environment in which all insurgents must operate.

A. INTERNAL INSURGENT COMMUNICATIONS

Every insurgent group is faced with the need to communicate. From the everyday orders and directions issued from the junior leaders of the organization to the strategic goals promulgated by the leadership, each underground organization is faced with the task

of sending and receiving messages, both on the individual and collective level. The ability to communicate successfully can mean the difference between an inefficient and soon-to-be nonexistent organization and an entity that triumphs to lead a nation. The insurgents must balance the inefficiencies of running an organization that is highly secretive on the one hand while creating an organization that is effective on the other.[1] This process evolves through an interactive process with uncertainty brought on by the actions and reactions of the government as well as those whom they are attempting to govern.

There are numerous environmental factors that play a role in an insurgency struggle and have an impact on its organizational development. The first and foremost is the security of the organization. Unlike any other organization, a guerrilla force must constantly be concerned for the safety of its individuals as well as organizational security and safety. Insurgent organizations operate in a hazardous environment, with governments continuously attempting to eliminate them through arrest, expulsion, and/or death. The business world, which may concern itself with the security of property rights or trade secrets, deals with security issues that pale in comparison to the life and death struggle that the guerrilla faces. The possibility of death permeates every rebel action from day to day living arrangements to the strategic planning of the organization. While secondary to the constant security concerns, there are other elements that influence the guerrilla's organizational life.

[1] Bell, J. Bowyer. "Aspects of the Dragon World: Covert Communications and the Rebel Ecosystem," International Journal of Intelligence and Counterintelligence, Volume 3, Number 1.

The means by which a society communicates as a whole also affects the insurgents' organizational environment. Communications can range from the person-to-person variety found throughout less-developed nations to the technology-rich environment found in highly industrialized parts of the world. Guerrillas can only use the means available within their working environment to communicate throughout their organization. The use of information technologies by only rebel elements of a society acts as an indicator to the guerrillas' identities. Insurgents spend much of their time attempting to blend into the society around them and are therefore restricted to the information tools available to other members of the society. Thus, the internal conductivity of a society plays an important role in the tools that the rebels have at their disposal.

Uncertainty is a constant reality in an insurgency struggle. The very nature of the struggle is based on the attempt to overthrow the existing government. Although many actions and reactions may be predicted or assumed in any adversarial endeavor, their certainty in degree and scope can have an impact on the insurgency in both positive and negative ways. Because of the uncertain environment, more information is needed to drive the decisions and actions of the organization. However, more information requires more security risk. The insurgents are therefore faced with two environmental factors that work against each other. On the one hand, the uncertain environment requires more information, and on the other hand, gaining more information means risking security.

The first effects of information technologies on an organization are likely to be felt at the top. The leadership, or as Henry Mintzberg labeled it the "strategic apex",[2] will be changed with the implementation of information technologies. The sheer amount of information available at the highest levels of an organization has the potential to be overwhelming. The strategic apex is faced with a choice between drowning in a sea of information or adapting the structural form of the organization to this newfound resource.

There are many routes an organization can take to deal with this potentially overwhelming influx of information. The one chosen depends upon the individual leadership of the organization. Leaders who are driven by high power and control needs are less likely to decentralize the decision process. Mintzberg mentions that besides the "information overload" scenario there exists two other main reasons for decentralization: 1) it allows the organization to respond quickly to local conditions; and 2) it is a stimulus for motivation[3]. Both these reasons are applicable to the insurgent organization with its desire to out-govern the standing government and to end the time of living as hunted individuals. The amount of decentralization, however, is dependent upon how much power a leader is willing to concede to his subordinates.[4]

Whether an insurgent group is centralized or decentralized is in many respects dependent both upon the individual leadership of the group and the motivations behind the

---

[2] Mintzberg, Henry, Structure in Fives: Designing Effective Organizations, Prentice Hall, Englewood Cliffs, N.J., 1993, p. 9.
[3] Mintzberg, pp. 96-97.
[4] Burton, Richard M. and Odel, Borge. Strategic Organizational Diagnosis and Design: Developing Theory for Application. Kluwer Academic Publishers: Boston, 1996.

group altogether. Organizations whose strategic thoughts and directions come only from one individual are less likely to decentralize. There is a core, or inner circle, of colleagues that may influence the leader, but rarely is the decision process truly open to the junior leadership of the organization.

On the opposite end of the spectrum are those organizations motivated by a central theme such as nationalism or separatist ideology; they are much more likely to decentralize in the face of overwhelming information flows. When an organization and its individuals are motivated by a common, agreed-upon theme, there is much more latitude for decision making because of the shared expectation that any actions of individuals will be in line with organizational goals.

1. The Factors That Influence the Use of Information Technologies by Insurgent Organizations

It can be deduced from this discussion that three factors influence the use of information technologies by an insurgent organization. These three factors--internal conductivity, leadership, and the information threat posed by the standing government--are discussed in further detail below.

a. Internal Conductivity

Internal conductivity is the type and amount of communication that occurs within a society on a daily basis. The internal conductivity of a society will be a strong determinant as to whether an insurgent group is likely or not to employ information technologies to meet its organizational demands. This should not imply that every

household of a society has to be hard wired before information technologies will be employed by insurgents, although a completely wired nation could greatly aid rebels in their day-to-day communication needs. Societies that already possess a vast wealth of information tools provide insurgents with a rich set of available weapons to meet their communication needs. These societies also present environments in which the insurgents' communications are more likely to get lost in the plethora of messages, or "noise," that is transmitted daily. On the other hand, societies with antiquated or slowly developing information tools may be more vulnerable to, and susceptible to, sudden exposure to new information technologies, but their long term uses open the insurgents to the reactions of government forces.

b. Leadership

The leadership of an insurgent organization is a determining factor in how information technologies will be employed by a rebel group. Besides the limitations of his own technical experience and competence, the potential future statesman also must contend with how much power he is willing to relinquish in the pursuit of the organizational goals.[5] The leader of an organization may be willing to relinquish a vast amount of power in the initial stages of an insurgency to gain notoriety and popular support for his cause. However, as the likelihood of success grows, the leader may consolidate and centralize many decisions to insure that only those truly deserving are

[5] Burton, Richard M. and Odel, Borge. Strategic Organizational Diagnosis and Design: Developing Theory for Application. Kluwer Academic Publishers: Boston, 1996.

offered the rewards at the end of the battle.[6] If an insurgent group does employ information tools to meet its communication needs, the organization is likely to be decentralized and more greatly dispersed. A decentralized organization is likely to be smaller and more professional then its centralized counterpart. The will, goals, and aspirations of the insurgent leadership has always been, and is likely to remain, an important factor in determining the extent to which a rebel employs information technologies.

c. Security Threat

Because of the security risk that every rebel lives with on a daily basis, the security threat that the government forces pose against information tools will have an impact on the likelihood of their use. No information tool is as important as the continued existence of the organization. The use of information tools is likely to become a cat and mouse game between insurgents and the state. Insurgents will use a peculiar information technology until the threat of exposure or compromise becomes so great that they are forced to move to another tool to meet their communication needs. Thus the disparity between the states' information technologies and the insurgents' becomes paramount. States that hold an edge in the use of information tools are likely to be able to identify, eliminate, or counter an insurgent group's undeveloped information technology much more quickly. On the other hand, insurgents who hold a technical advantage are likely to be able to employ the same means to communicate for a much longer time before changing.

[6] Notes, "Seminar on Guerrilla Warfare" at the Naval Postgraduate School.

The three factors identified above as determinants of how information technologies meet the internal communication needs of the insurgent organizations will be added to the framework. These factors will play a significant role in determining to what extent information technologies will meet the organizational communication needs of the insurgents.

B. COMMUNICATING WITH THE STATE'S POPULATION

There is no other resource as important to both the government and a struggling insurgency as the support of the people. All things being equal, the greater the popular support for an insurgence, the more effective the organization. Ernesto "Che" Guevara, a renowned insurgent from the late 1950s until his death in 1967, said, "to try and carry out [a guerrilla war] without the support of the population is a prelude to inevitable disaster."[7] The support of the people for a revolutionary cause has claimed the governing rights of states such as China, Iran, and, more recently, Poland. The step from disgruntled populace to revolutionary force is not an easy one. The "will" of a state's population must be captured and used as an instrument to change the governing apparatus. As political scientists such as Theda Skocpol[8] and Chalmers Johnson[9] debate the origins and causes of revolution, a new instrument has been developed that may aid rebel organizations in garnering popular support.

Prior analysis of state revolution has concentrated on the specific cultural and

---

[7] Guevara, Ernesto, Guerrilla Warfare, Lincoln: University of Nebraska Press, 1985, pp. 48-51.
[8] Skocpol, Theda, Social Revolution in the Modern World, Cambridge: Cambridge University Press, 1994.
[9] Johnson, Chalmers, Revolutionary Change (2nd Ed.), Stanford: Stanford University Press, 1982.

societal attributes that significantly contribute to changing a state's governmental status. Although the study of cultural characteristics remains important to the discussion of any particular revolution, a study at the macro level, such as this one, must step back to analyze causes that have promoted change across the entire spectrum of state systems.

The following discussion is restricted to factors that can be found across cultural and political ideological lines in order to determine where the use of information tools may aid the state or insurgents in an internal war.

An underground organization attempts to solicit support for its cause among a state's population. The insurgents attempt to promote and articulate a vision of how a state will run under rebel leadership. To do this, the rebels essentially attempt to out-govern the government. The insurgents use rhetoric that disparages a standing government while inflating their own successes. This disparaging rhetoric is designed to tear down trust, confidence, and support for an existing government while glorifying and magnifying the attributes of the underground organization. This is one area where the insurgents hold an advantage over a standing government. Confidence for a standing government is based on the government's bureaucratic actions. Confidence in a guerrilla organization is based a theoretic vision. Realities usually tend to be much harsher than dreams.

Attempts to influence a state's population take on different characteristics depending on which element, the standing state or insurgent organization, is attempting to influence the populace. The insurgents must change the status quo. This need to change

an already standing system implies that the rebels must take aggressive or offensive action to promote or change a citizen's allegiance. Popular support equates to resources for an insurgency. Added resources can come in the form of financial aid, equipment, or the simple silence of the populace when faced with an order from a standing government. This need to be aggressive by the insurgents gives them reason to use any means at their disposal. Failure will result in the destruction of the organization.

The state, in its attempt to control the population, must hold onto the status quo. Its actions toward the populace are fundamentally more defensive in nature. A state strives to quench, not inflame, the revolutionary passions of its constituents. This should not imply a passiveness or apathy toward the citizens. The population can hold vital pieces of information that the government can use to "see" the insurgents as well as other resources that are essential to the government in its war campaign. A supportive populace is the best defense for a struggling government. Aggressive or cruel treatment toward a member of the state by governmental representatives is likely to receive ample publicity from the struggling insurgents. This negative publicity does not have to be truthful to meet the needs of the guerrillas.

How a state's population communicates internally will determine how and if information technologies can be used to promote the beliefs and causes of both the standing government and an insurgent organization. Internal communications can range from the jungle grapevine that existed in Vietnam to the interconnected, hard-wired, multiple media found within many industrial countries. In societies where vast sources are available to reach and influence citizens, insurgents can pick and choose the mode in

which they attempt to connect potential followers. These multimedia societies provide insurgents with an ability to alter the means used to communicate with citizens, allowing them to vary their approaches based on a medium's security. In societies where the information sources are antiquated, the ability of the guerrillas to change attitudes by using information technologies is much more limited. A computer in the hands of rebels that is unable to communicate with any other citizens' computers is useless. Likewise, a government that has the ability to track cybermedia is useless if the guerrillas do not possess or use this capability. In these situations rebels may have to rely on the face-to-face communications found in many portions of the underdeveloped world.

The day-to-day interactivity of government representatives and the society can also affect whether information technologies are likely to be useful to a revolutionary cause. The interactivity can be as simple as police officers in the streets, infrastructure under construction, or any activity that demonstrates the government is working for the community. Any state in which the efforts of a government are easily identifiable to its citizens is less likely to be affected by disparaging information spread by rebels via sophisticated information tools. There is a tension, however, between the amount and type of exposure the citizens have to a standing government. Exposure of the government to the populace provides ample opportunities for an overaggressive or simply negligent act by a civil employee to be amplified by an advertising rebel. This concept implies that in areas of a country where the government presence is less dominate, insurgents are much more likely to be able to influence the local population.

The type of governmental system also plays a role as to how and if an information tool can influence a society. An open government, one that is developed through an electoral process, will be less likely to be affected by advances in information technology within its borders. These societies express their opinions at the ballot box. Information technologies used efficiently have the potential to overwhelm a population with information. Tools such as the Internet provide a resource where almost any type or amount of information can be found on any subject. In a society where free speech is the norm, citizens build up an immunity to negative government information. Likewise, in societies where negative government press is forbidden, a seemingly minor government indiscretion publicized by an insurgent is likely to have a greater impact. All things being equal, the more open a society, the less likely the impact of information technologies.

1. The Factors That Influence the Insurgents' Use of Information Technologies

Two main factors determine the use of information technologies to influence a state's population by an insurgent organization:

a. Availability of Information Technologies to a State's Population

The introduction of an information technology by insurgents that is not available to the remainder of a society serves no purpose. The only tools available for use by insurgents are those that are already present within a society at large. This factor can be determined by looking at the standard ways in which a state's citizenry obtains its daily news. Information tools range from the Internet-connected computer to a clandestine radio station that beams a revolutionary message to possible supporters. In a society that

receives its information via word of mouth, insurgents have little choice but to spread their revolutionary rhetoric via the same means. In societies in which there are limited types of technologies that are used to distribute information, insurgents face limited means to espouse their rhetoric.

b. Government - Society Interactivity

There is variability in the amount and type of interaction between the society at large and the government. If the insurgents' information can be distributed unhindered, government-society interactivity has an impact on that information. In a society in which government representation is apparent on a daily basis, the insurgents face a tougher, although target rich, opponent. The omnipresent state stands as a more formidable opponent. The state's ability to communicate with a society and receive feedback from constituents allows it to paint a more accurate depiction of underground activity. This government-society relationship is essential to the insurgents' ability to affect a population with its rhetoric. Although these states may stand as more formidable opponents, they also provide a target-rich environment for struggling insurgents. Overzealous acts by government officials can be used to support the insurgents' cry for a change in the government. The respect, or lack thereof, for government officials within a society is an indicator of the likely effects of information spread by insurgents to the society at large.

2. The Existing Government and the Use of Information Technologies

Two factors determine the likely effects of information technologies on a state's population by a standing government:

a. Government Responsiveness

The ability of a government to respond to disgruntled members of society determines the likelihood of its successfully using information technologies in its battle against insurgent forces. The feedback a government receives, no matter the source, is worthless unless it can react to it. Responsiveness, or the illusion of responsiveness, allows the government to give the impression that it is working for a society. Although responsiveness may alleviate some of the short-term pressure a government experiences, the long-term expense in terms of government resources can potentially aid insurgents in wearing down the stronger adversary. If there is no mechanism for responding to disgruntled members of a state, a government stands ripe for the insurgents' actions and the information tools they employ.

b. Political System

This factor refers to the type of political system already in place and the amount of openness within that system. Whether a state's political system is open or closed determines a government's ability to respond adequately when information technologies are used by insurgent forces to influence a state's population. An open government is likely to possess some skills in managing its own image. Disparaging information, no matter the source, is likely to be addressed and countered in a society where a government stands accountable to its public. A closed system, in which disparaging information against the government is not allowed, will not respond adequately. If a government normally has open discussions of its policies, it develops the

skills and attributes that will be essential if the insurgents' information barrage develops. Systems that do not face criticism on a regular basis are likely to be overwhelmed if a revolutionary information barrage begins. These governments possess an inclination to lash out against disparaging information, an act that has the potential of aiding an insurgent movement by providing information that can be used against the government.

C. COMMUNICATING WITH THE INTERNATIONAL COMMUNITY

Both belligerents, the state and the insurgents, bid for legitimacy and recognition within the international community. Although not a prerequisite for success, international recognition and support can have an enormous impact on the likelihood of success. One only needs to contemplate the outcome of the American Revolution without French support or the consolidation of Vietnam without the aid of the U.S.S.R. to appreciate the importance of international support. Although the need for support has always been a significant factor in the outcome of an internal war, today's information technologies provide greater opportunities for both parties to influence the international community.

This research confines itself to the internal conflict that consists of a state government and internal insurgency. This study does not venture into what Larry Cable defines as "partisan war," in which combatants from a third nation are used to conduct the conflict within a nation.[8] This notion would significantly cloud the analysis, although the basic factors would remain the same. With this restriction in mind, the influential factors are discussed below.

---

[8] Cable, Larry E., Conflict of Myths: The Development of American Counterinsurgency Doctrine and the Vietnam War, New York University Press, 1986, p. 5.

The insurgents and the state compete for legitimacy within the international community. The insurgents attempt to garner international support for their cause and for recognition. The government also attempts to solicit support, which would allow the government greater freedom of action to combat the insurgents. Both parties attempt to present a favorable image of their respective organizations and insure that their story is told in the most sympathetic manner.

The government and the insurgents both attempt to manage their images in order to put the most respectable light on their actions. Early in any insurgence, the state uses terms such as "outlaws," "criminals," and "terrorists" to convey to the world that the disturbances are of a criminal nature and not political. Using terms that convey criminal images to the international arena lends credence to the state's claim that its responses are justified to uphold law and order. On the other hand, the rebels use terms such as "freedom fighters" and "insurgents" to promote an image of justification and legitimacy. Both parties try to manage their respective images to present the most positive picture of the situation. Managing the perceptions of the conflict is accomplished through the information that flows from the besieged region and is received by the international community.

The type and amount of information that flows from a state under siege is a relevant element in the presentation of the belligerent group's image to the international community. Large amounts of information from multiple sources offer a more accurate picture of the situation within an embattled region. Numerous sources of information add credibility to a particular side of a story. However, areas in which source-rich and

quantity-rich flows of information collect are less likely to be influenced by the impact of a new source. In a high "noise" environment, a new source is more likely to get lost or diluted by the multiple counter arguments already present. States where a monopoly on public information is held (such as a government-administered news agency) are much more susceptible to the likely effects of information technologies. Freedom of the press doesn't necessarily promote multiple sources of information. Societies that possess monopolized information are more likely to be susceptible to the introduction of information technologies that have the ability to overwhelm the already present single information source. Likewise, states where information is distributed from multiple sources are less likely to be severely impacted by new information tools.

The state and the insurgents do not start on equal terms in terms of credibility of the information source. Few, if any, sources are held as more credible than the head of a state presenting a personal interpretation of an event. The legitimacy of an individual, a position, and a nation are all rolled into the words and actions of one talking head of state. A state leader will always be initially more credible than any insurgent. However, information technologies provide a tool that allows for a more open debate, one that can narrow the disparity between the head of state and the insurgency leader. Today's insurgency leader can enter a domestic debate from anywhere in the world, providing him with an over-the-horizon capability while he remains relatively secure. Information technologies, especially networked computers, allow insurgency leaders to debate relevant issues or express their individual and group proposals to a society. News conferences

with multiple media attendees organized by insurgent groups was an unthinkable prospect in the past due to security concerns by the secretive organizations.

Multiple sources of information include more than just the government and the media. Non-Government Agencies (NGOs) and Private Organizations (PVOs) also provide information. NGOs and PVOs have developed a networked capability that allows for greater and faster information flows into many less-developed portions of the world. A globally connected NGO may be the sole source of information flowing from an embattled state to the international community. Short-term technologies provided by visiting NGOs or the introduction of minimal technologies could have an overwhelming effect on a conflict where both the insurgents and the state hold little information technology maturity. Beyond the sources of information technologies introduced by outsiders, the information resources already present within a country play a significant role in the quest for international attention.

The information technologies available within a state under siege have a significant impact on their use and thus the outcome of a conflict. States that have no or limited exposure to informational technologies are regions where the effects will be felt more deeply. This holds true for both a society, of which the insurgents are a subset, and for government elements. This technology ratio between a society and its government presents another factor that should be analyzed to understand the impact of using information tools in a conflict.

Information technologies are a by-product of advanced business practices. The three entities--local business, society as a whole, and government--do not advance in their

uses of information technologies at the same rate. If both the government and society have advanced in their uses of information technologies at generally the same rate, no comparative advantage can be gained from the use of information technologies. However, if the society has advanced farther in its uses of new information tools than the government, then the insurgents are likely to hold a comparative advantage. If neither the government or business has advanced to any significant level, the sudden introduction of information tools by either side could have a large initial impact. Still, if a technology is not present, this does not prevent the use of cut-outs or other elements operating outside the state's borders to attempt to influence the international community from afar. Again, this over-the-horizon capability provides both an immediate expansion in the insurgents' capabilities while providing little denigration in their organizational security.

The ability to cause quantifiable, credible information to flow to the international community is essential to either the state's or the insurgents' capture of international attention and legitimacy within the world community. Three factors for both the insurgents and the state are presented below to analyze the potential impacts of information technologies on the battle.

1. The Insurgents' Use of Information Technologies

The following three factors should be considered when analyzing the effects of information technologies in an internal war. These factors are important to both parties involved in the conflict: the insurgents and the state in their respective attempts to acquire international support.

a. External Connectivity

External connectivity encompasses the ability of information to flow from and to the region in conflict. This can be studied in terms of purely technical conduits, such as external communication lines, or in terms of the exposure of the region to members of the international community, the individuals from the world community who pass through and expose the internal society to new technologies. The higher the conductivity, as in more outside lines or more exposure to the international community, the higher the likelihood that the international community will receive and be influenced by the information from the region.

b. Sources of Information

The number of sources of information operating from a region affects the credibility and potential influence of the insurgents' offerings. The larger the number of sources, the less likely the insurgents will be able to influence the information's credibility. A single-source society is an easier target for credibility attacks by the insurgents. The more information available from a region, whether true or false, the more noise is added to the system, which increases the likelihood of the insurgents' information being diluted. The lower the number of sources, the less noise, and the more likely the insurgents can have a significant effect on the presentation of the conflict. The insurgents in a multisource information environment must provide more credible information than the government's sources, which have an initial advantage in credibility.

c. Society/Government Technology Ratio

The society/government technology ratio describes the disparity between the insurgents' information capabilities and a standing government's. A government possesses advantages not afforded to the insurgents. However, information technologies provide an ability to flood the international community with information that has the potential to favorably influence world opinion. Flooding the world community with positive information provides the insurgents with political maneuvering space that may limit the physical response a government takes toward them. Information favoring the insurgents in an internal conflict can severely hamper the options a government can take. A government with as high an information technology capability can counter and dilute much of the information distributed by the insurgents and thus eliminate it as a tool in the guerrillas' arsenal. Again, the higher the society/government technology ratio, the more susceptible the government is to information that can damage its legitimacy in the international community.

2. The Existing Government's Use of Information Technologies

a. Sources of Information

The number of information sources communicating from a region affects the credibility and potential influence that an influx of government information may have on a conflict. The higher the number of sources within a society, the less likely that the government will be affected by the use of information technologies in an internal war. The more societal sources of information, the more scrutiny a government comes under on a daily basis. The addition of a new source in an already overflowing information system is

likely to have little effect. This new information may dilute the information already present, but it is unlikely to provide the ability to earn the legitimacy desired. A free press is a likely indicator of multiple sources of information; however this does not account for the monopolized information systems that are present in many parts of the world. In societies that have only limited numbers of information sources, as in only one newspaper, or one or two official news agencies, the likelihood that emerging information technologies will have a significant impact remains a higher possibility.

b. Government/Society Technology Ratio

This factor addresses the disparity between a standing government's information capabilities and the insurgents'. The government does not have to hold an advantage in this ratio to negate the effects of a robust insurgency information technology advantage. The government is afforded some advantages that the insurgents are not afforded in the world community. As long as a government has the capability to dilute the insurgents' influx of new information, the government will win out in the long run with the advantages afforded to the state in the world community. How high this ratio needs to be is directly relevant to both the individual state and the insurgent group. States that hold a higher and more creditable standing in the world community will require this ratio to be lower for this factor to affect an insurgency campaign.

c. Government Exposure to International Community

This factor looks at the standing and credibility a government possesses within the world community. Exposure to the world may be a result of a natural resource or geographic position in the world. Great economic powers are more likely to possess

the capability to discredit or nullify disparaging information presented by the insurgents within its borders. The more interaction with the world community, the more opportunities a standing government has to build on its quest for legitimacy. This exposure is built over time as the legitimacy of a government and its governmental system are solidified in the world community through consistency and years of interaction. States that remain isolated or do not possess a natural resource that is wanted by the world community are less likely to enjoy international exposure. Less exposure equates to less legitimacy and thus becoming a more likely target of the effects that information technologies have in denigrating the legitimacy of a standing government.

D. THE STATE GOVERNMENT VERSUS THE INSURGENTS

The battle that takes place between the state and the insurgents is a one-on-one confrontation unlike the struggle waged through the proxy of a state's population or the international community. This confrontation takes on many of the characteristics of a classical military confrontation pitting the insurgents against the military or police forces of a state. The militarily superior state attempts to search out and destroy the insurgents, who attempt to remain unrecognized until the time and place of their choosing.

The two parties of the conflict take on different characteristics in the battle for power. The state acts aggressively. The offensively oriented state gathers intelligence to identify the rebels within its citizenry. Once identification is accomplished, combating the under-armed and ill-equipped rebels is done easily. Segregation, isolation, and other techniques are used by government forces to eliminate the insurgent force. The insurgents act passively, attempting to remain anonymous to their counterpart. Successful guerrillas

only appear at the times and places of their choosing. These times and places are usually when the rebels hold a distinct advantage over governmental forces. These offensive and defensive characteristics are in many respects transferred to the information technologies that each party employs.

The insurgents' use of information technologies is determined by their need to defend themselves. Systems that allow an insurgent to communicate while not divulging his identity will take precedence over systems that merely pass information. Security within a system, safeguarding sources and identities, is more important than the comfortable redundancy of duplicate systems. Once an information technology has been exposed as a revolutionary tool, a rebel organization is likely to shift to a different technology to remain transparent to government forces. Which system the insurgents will choose depends upon what other systems are available within a society. With the explosion of available information systems throughout the world, insurgents face a future in which their choices are multiplying.

To a government, the security of individual identification within a system is of little importance. However, the interruption or denigration of an entire information system remains of paramount concern in the midst of an internal conflict. An information system hindered by a guerrilla attack affects a state's ability to govern as well as its legitimacy in the eyes of its constituents. With redundant systems, little denigration occurs in government services. Slight inconveniences are likely to be tolerated by a society; the complete loss of services will not.

Information technologies that aid the government or the insurgents are not without their limitations. Dependence on any single information system indicates a vulnerability, a necessity for use in the accomplishment of some organizational task. This necessity, and thus the system itself, presents a healthy target for any adversary. Set aside any disbelief in the possibility, and imagine the destruction to our government's prestige if every information system within the Social Security Administration failed to work. Reliance instills habits. Habits are the nature of bureaucratic work. Asking a government service employee to adapt to a disruption in an information system is preparation for inevitable disaster.

Even an adaptive organization, however, is hindered by changes or disruptions to its information systems. A worker or organization that is continually changing or rectifying system errors will naturally become reactive rather than proactive. When a government faces an adversary that is allowed to pick the time and place for confrontation, it must continue to strive to remain proactive in the face of such misfortune. Adapting information systems in the midst of confrontation forces either a government or the insurgents down a reactive path, which is a sure indicator of disaster.

The reliance on intelligence is essential to the government's ability to identify a rebel force within its society. Information technologies that collect, collate, and even decipher data will provide a state with a much-needed weapon in its arsenal. If this data is available, it will offer a state an accurate picture of a secret organization's traits. However impressive redundancy in itself may be, organizing it remains a key to a state's

intelligence-gathering machinery. Data not collaborated becomes vulnerable to vicious actions against a state's security apparatus.

The civil liberties held sacred within a society can also affect the extent to which information technologies can have an impact in an internal war. Whether it is the freedom of the press, freedom of speech, or the privacy of individual citizens, any civil liberty valued by the people can affect the means by which both the insurgents and the government attack their adversaries. These civil liberties may limit the ability of a government to crack down on its individual citizens. Likewise, these civil liberties may provide the legal basis that the rebels may hide behind as they broadcast their revolutionary rhetoric. The mere presence of such liberties is not enough to hinder a government's response, however, as numerous countries have temporally suspended liberties in the face of confrontation.

Based upon the characteristics of a direct state versus insurgents battle, the factors that are likely to influence how and when information technologies will affect a particular internal struggle are discussed below.

1. The Direct Battle Between the Insurgents and the State

The following two factors should be analyzed to determine what impact information technologies may have in any particular internal war. These factors are relative to the two parties involved in the conflict: the insurgent group and the state in their struggle for power.

a. Dependence on a Particular Information Technology System

The dependence upon one information system by either the insurgents or the government is not only an indicator of its use but also determines any counter uses within a conflict. A technology used before a conflict will likely remain in use once a conflict ensues. If this tool is used over an extended period of time without mishap or compromise, there will be a built-in dependence for that particular system. A dependence by either belligerent provides a target that may be too important to ignore. If the skills to counter this technology are not present within an organization, then the capability to out-source and hire the necessary intellectual and individual resources will surely exist. Back-up systems are a necessity. Surprisingly, the inability for government bureaucrats to adapt to new technologies may provide some built-in redundancy for the government. A government slow to move to emerging technologies or hesitant to give up old practices provides some protection against catastrophic attacks on particular information systems. The time and extent of use of a particular system will determine the degree of dependence. The longer the practice and greater the extent, the larger the impact of disruption.

b. Civil Liberties Adhered to Within a Society

If the above criteria describe those environments in which the use of information technologies present likely targets, this factor addresses how those targets may be attacked. Every society lies somewhere between total freedom and total oppression, where the concepts of freedom are simply not present. To determine the presence and impact of this factor, one cannot take government policy and laws at face value. A study must look at the governmental practices and its reactions under pressure to

determine how this factor will affect an internal war. In societies where civil liberties are the norm, the insurgents will be able to hide behind many of the government's own systems to achieve some freedom of action. However, once this freedom encroaches on the freedoms of others, a government's reactionary process should be studied to determine how it can be used by the insurgents. In societies where civil liberties are not the norm, a government's over-zealous use of force can be a tool through which the insurgents ignite internal decent. Whichever the case, the civil liberties within a society play an important part of when and how a government reacts to dissent within the society.

The two factors identified above as well as the others identified previously in this chapter will be added to the framework presented earlier in Figure 2.

E. CHAPTER CONCLUSIONS

The factors that will influence the use of information technologies in any ongoing or future internal conflict have been discussed and identified above. These factors are added to the framework presented earlier, and the results are shown in Figure 3 below. These factors can be studied to determine the extent to which information technologies can influence the outcome of any particular insurgency.

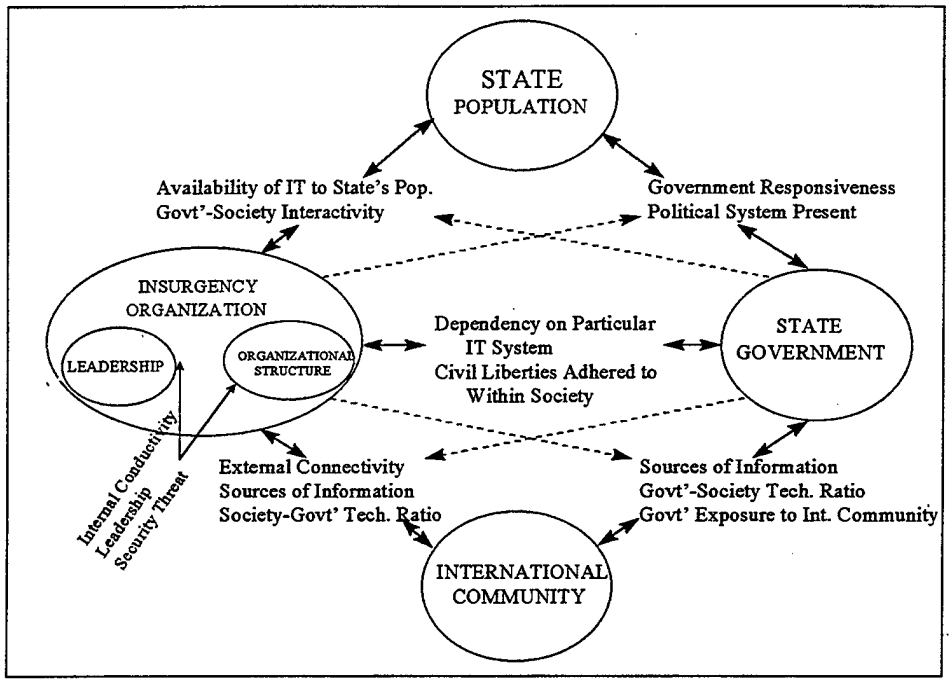

Figure 3. Influential Factors in the Use of Information Technologies

Involvement in any future guerrilla campaign as a participant will be undertaken from one of two perspectives: as an insurgent or as a supporter of a state government. A supporter of a state should study the factors identified along the lines that emanate from the state government portion of the diagram above to determine where susceptibilities and capabilities exist in any struggle. Analysts as well as participants should study the opposite portion of the diagram, from the insurgents' perspective, to identify strengths and weaknesses in the insurgents' attempts to influence both the state's population and the international community. This analysis can be used to determine how a state may disrupt, as shown on the dotted arrows above, any attempt by the insurgents to use information technology to aid in their attempt to undermine the standing government.

The list of factors identified throughout this chapter is not designed to be an all-inclusive list. Factors that arise based on specific conflicts, because of cultural or societal conditions, should also be added and incorporated into any analysis. It must also be remembered that the true impact of the influences of information technologies on societies as a whole is far from complete. As information tools are developed and implemented by societies, this framework should be reexamined to identify relevant emerging factors.

III. APPLICATIONS TO THE FUTURE

The factors identified in Chapter II are a starting point in the analysis of the impact of information technologies on future internal conflicts. These factors, however, are largely dependent upon the adversary a government or insurgent group faces. Discussions throughout Chapter II indicate that having either a robust or nonexistent information technology capability is directly relative to the capabilities of your opponent. This chapter will go one step further, beyond identification of factors, to determine in which situations it will be in the best interest of a belligerent force to implement certain characteristics of an information technology strategy. In which situations does the relative advantage lie in implementing an offensive and in which a defensive information technology strategy?

A. THE UNEVEN FUTURE BATTLEFIELD

The future insurgency battlefield will take place on uneven technological ground. The future, like the past, will present conflicts in which one side of a struggle will hold a technological advantage over an adversary. Like conventional weaponry, information technology is an asset, the possession of which provides some relative strength to its user. However, unlike with conventional weaponry, the extent of the advantage will be dependent upon the capabilities of the adversary. An information technology tool is only as effective as the target it is intended to be used against. A technology that passes millions of pieces of information not received by anyone is worthless to a user. An information tool researched, developed, and implemented that has no target consumes resources that can best be used for some other purpose.

Conflict is an interactive process. What may be successful against one adversary may be useless against another. Much like the environmental factors that are at play in

any conflict, the techniques and practices of one side of a conflict are always dependent upon the actions and reactions of the opposing side. For the U.S. military for instance, what was applicable in the jungles of Vietnam was not relevant in the deserts of Kuwait. The relative use and employment of information technologies also depends on the capabilities of the opposition.

What constitutes a high or low information technology capability? A frame for perception is necessary in order to analyze the relationship between belligerents with different capabilities in an internal conflict. The description below will aid in framing the perceptions and referencing the capabilities of either force. For a reader, a frame is necessary before further comparison of the capabilities and limitations of opposing forces is attempted.

The high technology force of the future will look much like the United States of today. The military, as well as the society at large, will possess a robust information technology capability. This capability will include multiple sources of credible news agencies as well as an interconnected society that can receive and respond to the information at large. The high-tech military of the future will incorporate many of the means to communicate within a society to further the military's command and control (C2) capability. This capability will include offensive measures designed to attack an opponent's communication and information capability. The force of the future will also possess a defensive capability designed to prevent the disruption of its own communications systems.

The low information technology society of the future will look much like the country of Somalia today. This society will possess little, if any, information technology

capability. Information will primarily be spread via word of mouth. Even the use of written language material will be limited by the literacy rate within the country. Besides the oral communications issued by military leaders, the signaling capability of a military source will include the antiquated means of beating drums or the use of signaling flags. Legitimate news agencies will be nonexistent, and the means to promote newsworthy issues will be limited in both scope and scale. This low-tech society will possess neither the aptitude nor the resources to incorporate any of the information technologies being developed throughout the rest of the world.

It becomes apparent that the majority of the states throughout the world fall somewhere between the U.S. and Somalia in their information technology capabilities. Whether the Western European states that approach the capabilities of the U.S. or the many underdeveloped states found throughout Africa, most countries possess some level of information technology capability. The relative information capability of any country limits both a government's and an insurgent force's ability to maximize the uses of information technologies in an internal conflict.

B. INTERACTIVITY BETWEEN HIGH-LOW TECHNOLOGY

Figure 4, shown below, indicates the relationship that exists between a high-tech insurgent force or state and a low-tech insurgent force or state. This graph lays out a foundation for the application of an information technology strategy relative to the capabilities that a government has and how they are affected by the adversary it faces. The graph addresses the strategy of a government's use of information technology as well as the nature of employment from a government's perspective.

		STATE	
		HIGH TECH	LOW TECH
INSURGENCY	HIGH TECH	Robust Offensive and Defensive Capability Speed of Application Essential	Offensive in Nature Outsourcing of Capabilities
	LOW TECH	Defensive in Nature Direct Off. Capabilities towards Inter. Comm.	Offensive in Nature Speed of Application Essential

Figure 4. Interrelationship between High-Low Tech Opponents

The figure above indicates that in a scenario in which both the government and the insurgents possess a high technology capability, both offensive and defensive capabilities must be emphasized. A government must protect its resources to defend against attack by an adversary. These defensive characteristics will include redundant systems, safeguards against exposure, and a tendency to be systematic in its approaches to the applications of information technologies. A government's offensive tools must also be employed as quickly as possible to force an insurgent organization into a reactionary mode. The speed with which either force employs an information technology capability is essential to realizing marginal returns before an enemy can counter and diminish a capability.

The sector that describes the low-tech government facing the high-tech insurgents indicates the use of a different strategy. The government should use all means at its disposal to implement its offensive capabilities. If these capabilities do not exist within a

government, then the bureaucratic organization should look to outsourcing this task either within the society or from resources outside its borders. Defensive concerns are negligible if a government possesses nothing to protect. A government in this situation should also leverage the advantages belonging to a standing government within the international community to influence world opinion in its favor. A low-tech government must not trade information inferiority for military force superiority. A government must guard against aggressive or violent reactions directed at its citizenry in an environment in which its opponent has the ability to advertise governmental indiscretions.

In the high-tech government against a low-tech insurgent force scenario, an emphasis on internal, defensively oriented information technologies becomes paramount. A government emphasis must be on the protection of standing information systems. The largest threat that the government faces is to the information systems that distribute and pass information as part of its administrative capabilities. Any offensive capabilities should be directed toward the international community to gain the freedom of maneuverability to combat the insurgents without international interference. An internal defensive strategy combined with an external offensive strategy is the optimal approach for a high-tech government facing a low-tech insurgent force.

The last sector of the graph demonstrates the confrontation between a low-tech state and a low-tech insurgent force. In this confrontation, any advantage that can be obtained from the use of information technologies can be maximized through speed. The speed in which a government employs a technology will determine the marginal returns of a particular information tool. Speed of application is not inherently a government strength. Levels of bureaucracy slow the time between decision and application. The

insurgents, who do not face such suffocating bureaucratic requirements, may be able to implement a technology in a more rapid manner. The speed at which each adversary applies a technology may provide an initial advantage that a late arriver finds hard to overcome, as well as maximizing the marginal returns of a specific tool.

The graph demonstrates that a standard use or approach to the employment of information technologies does not exist. Whether a government takes an aggressive offensive or defensive approach to the employment of information technologies is dependent upon the opposition it faces. When the returns from the employment of an information technology do not meet the costs of that technology, resources are not maximized. In a world in which stable or shrinking resources chase stable or expanding demands, the efficient use of resources must be maximized to meet the requirements of a national leadership.

C. CONCLUSIONS

This thesis has intenionally been left vague as to what constitutes an information technology. Mass media, interconnected computers, microprocessors, cellular communications, and similar advances have all changed not only the way a society communicates but also how it reacts to the overwhelming information available. The extent of this reaction and the further actions of a society are yet to be determined. The identifying of specific information tools has been left open so that this paper remains viable in an environment of constant change. Analysis of the true impact of information technologies on society will be a task for future historians. Constant analysis and anticipation of the impacts of information technologies in an environment of constant change is a requirement for effective policymakers of today.

This process has identified certain factors that can be used as a framework to determine susceptibilities and capabilities within the communication requirements of any internal conflict. Complete analysis of these factors, plus any developed later, can aid a government or insurgent group in determining where advantages may lay in any guerrilla war. These advantages or susceptibilities must then be viewed through the relative strengths and weaknesses of an opponent to develop a strategy toward the employment of any specific information technology. This process provides military and national leaders an approach to confronting the demands of insurgency conflict and how information technologies can affect the winner-take-all game for state power.

SELECTED BIBLIOGRAPHY

Bell, J. Bowyer. "Aspects of the Dragon World: Covert Communications and the Rebel Ecosystem," *International Journal of Intelligence and Counterintelligence*, Volume 3, Number 1.

Burton, Richard M., and Odel, Borge. *"Strategic Organizational Diagnosis and Design: Developing Theory for Application,"* Kluwer Academic Publisher: Boston, 1996.

Cable, Larry E. *"Conflict of Myths: The Development of American Counterinsurgency Doctrine and the Vietnam War,"* New York: New York University Press, 1986.

Guevara, Ernesto. *"Guerrilla Warfare,"* Lincoln: University of Nebraska Press, 1985.

Johnson, Chalmers. *"Revolutionary Change"* (2nd Ed.), Stanford: Stanford University Press, 1982.

Leites, Hathan, and Wolf, Charles Jr. *"Rebellion and Authority: An Analytic Essay on Insurgent Conflicts,"* RAND, February, 1970.

Metz, Steven and Kievit, James. *"The Revolution in Military Affairs and Conflict Short of War,"* Strategic Studies Institute: U.S. Army War College, July 25, 1994.

Mintzberg, Henry, *"Structure in Fives: Designing Effective Organizations,"* Prentice Hall, Englewood Cliffs, N.J., 1993.

Rose, John BG. *"American Army Introduction to the 21st Century,"* 1998.

Skocpol, Theda. *"Social Revolution in the Modern World,"* Cambridge: Cambridge University Press, 1994.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center.....2
   8725 John J. Kingman Rd. Ste 0944
   Fort Belvoir, VA 22060-6218

2. Dudley Know Library.....2
   Naval Postgraduate School
   411 Dyer Rd.
   Monterey, CA 93943

3. Professor Gordon H. McCormick.....2
   (Code CC/Mc)
   Naval Postgraduate School
   Monterey, CA 93943

4. Professor Erik Jansen.....1
   (Code MN/Ja)
   Naval Postgraduate School
   Monterey, CA 93943

5. Professor Dan C. Boger.....1
   Chairman, C3 Academic Group
   (Code CC)
   Naval Postgraduate School
   Monterey, CA 93943

6. United States Special Operations Command.....1
   Joint Special Operations Forces Institute
   Ft. Bragg, NC 28307-5000

7. Jennifer Duncan.....1
   Center for Special Operations
   (Code CC/Jd)
   Naval Postgraduate School
   Monterey, CA 93943-5000

8. US Army Command and General Staff College.....1
   ATTN: Library
   Ft. Leavenworth, KS 66027-6900

9. Maraquat Memorial Library.....1
   US Army John F. Kennedy Special Warfare Center
   Rm. C287, Bldg 3915

10. Maraquat Memorial Library.....1
US Army John F. Kennedy Special Warfare Center
Rm. C287, Bldg 3915
Ft. Bragg, NC 28307-5000

11. MAJ Joel J. Clark.....1
324 34th Street
West Des Moines, IA 50265