MASTER OF SCIENCE
IN
DEFENSE ANALYSIS

THE ILLICIT SMALL ARMS TRADE (U)

David A. Abernathy, II-Lieutenant, United States Navy
B.S., Naval Postgraduate School, 2000
Master of Science in Defense Analysis-December 2000
and
Lance B. Dettmann-Lieutenant, United States Navy
B.S., Naval Postgraduate School, 2000
Master of Science in Defense Analysis-December 2000
Advisor: John Arquilla, Information Warfare Academic Group
Second Reader: David Tucker, Command, Control, Communications, Computers, and Intelligence Academic Group

There are a variety of options that must be investigated when attempting to control the illicit Small Arms/Light Weapons (SA/LW) trade. This thesis weighs current control options via an economics-based analytic framework. Currently, solutions focus on three general areas of influence: *prevention of production; prevention of sales and purchases; and coercion to relinquish*. One can further delineate these areas of influence by looking at how these options could be best implemented—by *political/diplomatic*, *judicial (policing)*, and/or *military* means.

There are short and long-term consequences to any actions taken to try to control the illicit SA/LW market. In our opinion, the key to controlling the illicit SA/LW market is two-fold. First, along with today's focus on supply-side options, decisionmakers need to implement demand-side options, such as *social reconstruction* and *economic development.* This will remove the s*ecurity dilemma*—peoples' perceived need to maintain weapons for self-protection against internal and external threats. Second, when decisionmakers choose to implement supply-side solutions, they need to keep the market continually in a state of having to react to varied control measures in the short term. This can be done by periodically exposing the SA/LW market to new control measures that force it to constantly do business by different means.

DoD KEY TECHNOLOGY AREAS: Conventional Weapons, Computing and Software

KEYWORDS: Small Arms, Light Weapons, SA/LW, Weapons Trafficking, Counterproliferation, Black Market, Gray Market, Arms Sales

HOW TO DEFEAT INSURGENCIES: SEARCHING FOR A COUNTER-INSURGENCY STRATEGY?

Michael A. Bottiglieri-Major, United States Army
B.B.A., Texas A&M University, 1989
Master of Science in Defense Analysis-December 2000
Advisor: Anna Simons, Special Operations Academic Group

Most people say that a hearts and minds campaign is the best strategy for defeating an insurgency. But there may be no one best solution applicable to countering all insurgencies. The opportunities and constraints, which affect both the insurgent and state, dictate the best strategy. This thesis tests this hypothesis against the most difficult form of insurgency. Two Maoist insurgencies will be analyzed to determine the effect of the state's strategy on the insurgent. Conclusions will then be drawn about the relevance of pursuing a universal counter-insurgency strategy.

While countering the Shining Path insurgency in Peru, the state employed three different strategies. In the end, the state recognized that the insurgency was elitist-based and launched a successful counter-leadership targeting campaign to defeat the insurgency. While countering the Malayan Communist Party insurgency in Malaya, the state employed two different strategies. In the end, the state recognized that the insurgency could be limited to the ethnic Chinese community and adopted a successful campaign to separate the insurgents from the population.

Analysis of each case study clearly demonstrates the success of two different strategies against similar insurgent organizations. In Peru the insurgency was defeated thanks to an inside-out approach, while in Malaya the insurgency was defeated form the outside-in. The strategy used in Peru would not have been successful in Malaya and the same can be said of the Malayan strategy in Peru. However, the cases demonstrate the need to understand general counterinsurgency principles before applying case specific strategies. Based on these observations it can be concluded that, just as the principles of war guide military operations, there are similar principles which bring success in counterinsurgency operations, with the important caveat that every case must be treated as unique.

DoD KEY TECHNOLOGY AREA: Other (Counterinsurgency)

KEYWORDS: Counterinsurgency, Guerrilla Warfare, and Insurgency

REVISITING THE BATTLE OF THE LITTLE BIG HORN

Matthew J. Burns-Lieutenant, United States Navy
B.S., Naval Postgraduate School, 2000
Master of Science in Defense Analysis-December 2000
Advisors: Gordon H. McCormick, Special Operations Academic Group
Bard Mansager, Department of Mathematics

The Battle of the Little Big Horn has captured the interest of historians, scholars, and military enthusiasts since the day that over 200 United States soldiers under General George Armstrong Custer's command were decimated by Crazy Horse and 2000 Indian warriors. Competing theories regarding the details of the battle have arisen, mostly due to conflicting first hand accounts.

The purpose of this thesis is twofold. The first purpose is to perform an historical analysis of the Battle of the Little Big Horn, using war-gaming. A series of controlled, comparative simulations of the battle will be carried out using the Synchronization Matrix, a war-gaming tool obtained from U.S. Army Field Manual (FM) 101-5. This analysis will evaluate three competing theories and interpretations of the battle, with the objective of categorizing the theories by degree of plausibility. The second purpose is to examine the impact of alternative notional leadership decisions on the outcome of the battle, e.g. what if Custer had not split his force? The result is a confirmation that war-gaming can indeed be utilized for the study of historical combat, as well as for future planning.

DoD KEY TECHNOLOGY AREAS: (Other) Primitive Technology

KEYWORDS: War-Gaming, Course of Action Analysis

POLITICAL VIOLENCE IN EURASIA: RADICAL ISLAM OR RATIONAL ACTING?

Simon C. Gardner-Captain, United States Army
B.S., University of Massachusetts, 1985
Master of Science in Defense Analysis-December 2000
Advisor: Anna Simons, Special Operations Academic Group
Second Reader: Glenn Robinson, Department of National Security Affairs

Much of the violence in Eurasia since the break-up of the Soviet Union has been blamed solely on radical Islamic Fundamentalism. This characterization is at best simplistic and at worst dangerously insufficient. Misunderstanding the complexities of this instability will undermine efforts by diplomats and soldiers to prevent future violence. Poorly understanding this violence will likewise hinder U.S. and multilateral post-conflict operations. Given the high likelihood for continued instability and violence in this critical region, its causes and complexities must be understood, and applying off-the-shelf "lessons learned" from other conflicts must be avoided.

This thesis attempts to provide a framework to understand the complex socio-political underpinnings of societies in Central Asia and the Caucasus. The thesis dispels the popular notion that the preponderance of regional violence is purely predicated on Islamic fanaticism. Rather, through the use of three case studies of recent conflicts in the region, this thesis shows that political violence is largely the result of political entrepreneurs exploiting extant ethnic, national, and religious cleavages when opportunities arise. This violence is not representative of a deterministic "clash of civilizations." Only through understanding the fluid and malleable nature of this political violence can one craft meaningful engagement and post-conflict strategies.

DoD KEY TECHNOLOGY AREA: Other (Special Operations)

KEYWORDS: Ethnic Conflict, Islamic Fundamentalism, Central Asia, Wahabbism

UNMANNED AERIAL VEHICLES AND SPECIAL OPERATIONS: FUTURE DIRECTIONS

Gregory K. James-Major, United States Army
B.S., University of Washington, 1988
Master of Science in Defense Analysis-December 2000
Advisor: Gordon H. McCormick, Special Operations Academic Group
Second Reader: E. Roberts Wood, Department of Aeronautics and Astronautics

Advances in computing, miniaturization, imaging, and data transmission technologies are precursors to a more important role for UAVs in warfare. UAVs are likely, first, to revolutionize the way reconnaissance and surveillance are conducted, second, to increase the capabilities of small units, third, to join manned platforms in the conduct of assault and attack missions, and finally help provide the numerous nodes necessary to facilitate both the digital connectivity and swarming forces envisioned in future network-centric formations.

This thesis focuses on answering six questions:

-What missions can UAVs perform?
-What missions should UAVs perform?
-What type of UAV is appropriate for each mission?
-How can SOF use UAVs?
-Who should own the UAV (from a SOF perspective)?
-What level of control is required and where?

Results include what UAV missions and types could support special operations, which of these should be performed by UAVs organic to special operations, and which should be performed by the Services' UAVs, as well as recommendations for future command and control of UAVs supporting special operations. Results are presented in matrix form for easy correlation of related factors. The thesis concludes with a twenty-year prognostication of UAV development and recommends areas for future study.

DoD KEY TECHNOLOGY AREAS: Air Vehicles, Battlespace Environments, Command Control and Communications, Electronic Warfare, Sensors

KEYWORDS: Unmanned Aerial Vehicles, UAV, Special Operations Forces, SOF, Future of Warfare

DIRECTED ENERGY: APPLICATIONS AND VULNERABILITIES (U)

Alexander R. Merz-Captain, United States Air Force
B.S., Naval Postgraduate School, 2000
Master of Science in Defense Analysis-December 2000
Advisor: John Arquilla, Information Warfare Academic Group
Second Reader: David Tucker, Command, Control, Communications, Computers, and Intelligence Academic Group

Much has been made in recent years of the potential for directed energy (DE) to be used as a weapon, and of U.S. vulnerability to such modes of attack. This thesis surveys the current status of laser, high-power microwave, particle beam, and acoustic technology to answer two primary questions. First, what sorts of tactical DE weapons can be fielded in the next 10 years? Second, if developed, what sort of threat would these systems pose to the U.S.? Conclusions assess potential applications and threats of DE weapons in the next ten years and suggest areas for further research.

DoD KEY TECHNOLOGY AREA: Directed Energy Weapons

KEYWORDS: Directed Energy, LASER, High-Power Microwave, Radio Frequency, Particle Beam, Acoustic, Weapon

ORGANIZATION DESIGN PRINCIPLES FOR COUNTERING TERRORISM IN THE UNITED STATES

Matthew C. Mingus-Major, United States Army
B. S., Troy State University, 1990
Master of Science in Defense Analysis-December 2000
and
Richard D. Orman-Captain, United States Army
B. S., United States Military Academy, 1991
Master of Science in Defense Analysis-December 2000
Advisors: David C. Tucker, Command, Control, Communications, Computers, and Intelligence Academic Group
Susan P. Hocevar, Department of Systems Management

Recent terrorist activities (the World Trade Center bombing, the Oklahoma Federal Building bombing, the release of Sarin Gas in the Tokyo subway, etc.) have focused the national leadership on the topic of terrorism inside the borders of the United States. In response, two Presidential Decision Directives (PDD-62 and PDD-63) were issued to help define the terrorist threat and recommend a counter-terrorism organization in the federal government. However, the directives do not determine how the Federal government works with state and local authorities. The directives also do not focus on local, state, and federal capabilities to preempt a possible terrorist attack. This thesis builds a organizational framework of the U. S. counter-terrorism environment; explains the current U. S. counter-terrorism structure from a local perspective; develops a set of principles that could be used by any local or federal agency to develop a new or more efficient counter-terrorism organization; assesses two domestic counter-terrorism organizations; and proffers specific recommendations on how U. S. counter-terrorism organizations and programs could be more efficient.

DoD KEY TECHNOLOGY AREA: Other (National Security Affairs, Special Operations)

KEYWORDS: Counter-Terrorism, Domestic Counter-Terrorism, Terrorism, FBI, Interagency Working Group, Organization Design, Network

NAVAL SPECIAL WARFARE-LEADING ORGANIZATIONAL CHANGE

Robert A. Newson-Lieutenant Commander, United States Navy
B.S., University of Kansas, 1989
Master of Science in Defense Analysis-December 2000
Master of Arts in National Security Affairs-December 2000
Advisors: Gordon McCormick, Special Operations Academic Group
Ken Hagan, Naval War College

This thesis examines organizational transformation, utilizing Naval Special Warfare (NSW) as a model for DOD-wide organizational change. The broader context of the revolution in military affairs (RMA) highlights the unique role of special operations forces in general and NSW specifically regarding innovation and adaptation in the military and its diffusion to conventional forces.

Four elements: technological change, systems development, operational innovation, and organizational adaptation compromise a revolution in military affairs. Although technological change and systems development have made significant impacts upon military affairs, operational innovation and organizational adaptation are lacking. Organizational adaptation responding to information age realities–changing geo-political and social circumstances as well as rapidly advancing technology–is necessary to achieve the predicted revolution in military affairs. A transformation from a rigid hierarchical organization to a collaborative network of stakeholders is recommended.

Speed, agility, integration, and innovation are necessary success factors in the 21st century. In order to achieve these attributes, military organizations must leverage resources across hierarchal, functional, command, and social boundaries. This will require a long-term transformation effort.

DoD KEY TECHNOLOGY AREAS: Other (Organizations)

KEYWORDS: Organizational Transformation, Revolution in Military Affairs (RMA), Collaboration, Networks

THE GUNFIGHTER'S DILEMMA: MULTIPLE ADVERSARY DETERRENCE AND COERCION

Jess Palmer-Major, United States Air Force
B.S., United States Air Force Academy, 1985
Master of Science in Defense Analysis-December 2000
and
Mark Stebbins-Captain, United States Army
B.A., Princeton University, 1989
Master of Science in Defense Analysis-December 2000
and
Andrew Zacherl-Captain, United States Army
B.S., University of Oklahoma, 1991
Master of Science in Defense Analysis-December 2000
Advisor: John Arquilla, Information Warfare Academic Group
Second Reader: Gordon McCormick, Special Operations Academic Group

Throughout history great powers have had to wrestle with the problem of maintaining their influence over the world around them. Often these powers were simultaneously faced with more than one opponent. In order to meet multiple challenges, leading nations have had to maximize the number of potential adversaries they could influence with each action or policy.

Those faced with this dilemma have included the Romans, Byzantines, and the British Empire. Studying these nations in their struggle to maintain control revealed tactics and techniques that proved effective. Forward deployment, statements of perseverance, the use of coalitions, strategic distraction of opponents, and the demonstration of their relative superiority over adversaries all helped to preserve the longevity of these empires. Additionally, an effective information campaign, which amplified successes, proved invaluable to these world powers.

This thesis explores how a single action often affects more than just the two parties taking and receiving action. It then discusses the flow of how the information content of foreign policy actions transfers from the primary actor to multiple secondary actors. Historical cases of multi-adversary deterrence and coercion are used as models of how this hypotheses, coupled with a good information strategy, maximized the studied powers' effectiveness.

DOD KEY TECHNOLOGY AREA: Other (Information Operations)

KEYWORDS: Deterrence, Coercion, Information Operations

OPEN SOURCE TOOLS: APPLICATIONS AND IMPLICATIONS

Michael D. Stull-Lieutenant, United States Navy
B.S., United States Naval Academy, 1993
Master of Science Defense Analysis-December 2000
Advisors: John Arquilla, Information Warfare Academic Group
Timothy J. Shimeall, Carnegie-Mellon

The Internet provides users with unparalleled access to a wide variety of open source tools. Some of the tools may be used in conjunction with others or by themselves, often with great disruptive effect on a target. The rapid pace of discovered vulnerabilities in computer systems, along with the cooperation of expert programmers, has given users access to tools that lower the "entry costs" for conducting sophisticated attacks. Internet security is dependent upon reacting effectively to continually changing modes of attack, and is therefore almost always a step behind, in an action -reaction process.

The availability of pre-tailored attack codes gives possible enemies an avenue to attack the U.S. anonymously, with only a small investment of resources. However, attackers do still need both tools and the knowledge of how to use them to carry out most attacks. Still, more knowledge of the proper utilization of open source tools is progressively being coded into these open source tools, opening up the ability to conduct attacks to a higher percentage of the Internet population.

DoD KEY TECHNOLOGY AREA: Computing and Software

KEYWORDS: Internet, Open Source Tools, Computer Vulnerabilities, Information Operations