The Surprise Hypothesis

A Monograph
by

Major Mark J. Kneis II
United States Army

School of Advanced Military Studies
United States Army Command and General Staff College
Fort Leavenworth, Kansas
AY 02-03

SCHOOL OF ADVANCED MILITARY STUDIES

MONOGRAPH APPROVAL

Major Mark J. Kneis II

Title of Monograph: The Surprise Hypothesis

Approved by:

_____	Monograph Director
Jeffrey R. Witsken, LTC	
_____	Professor and Director Academic Affairs, School of Advanced Military Studies
Robert H. Berlin, Ph.D.	
_____	Director, Graduate Degree Programs
Philip J. Brookes, Ph.D.	

Abstract

THE SURPRISE HYPOTHESIS by MAJ Mark J. Kneis II, U.S. Army, 46 pages.

The Unites States dominates the conventional battlefield, but this power might prove to be a nemesis. This power forces enemies to seek capabilities that level or change the playing fields. Weapons of mass destruction and mass effect are indeed one way for adversaries to level the playing field, but there is another, surprise. Surprise transcends technology and budgetary concerns. The horrific events of 11 September are a reminder. Yet how well does the U.S. Army understand surprise? Do planners know how to plan for surprise operations? Terrorists do. Do planners know how and why surprise works? Adversaries seem to. There is much more to this principle of war than what military doctrine portrays.

Using the scientific method, this monograph combines the concepts of surprise and information superiority to create a hypothesis that explains the principle of war. The hypothesis rests on the belief that omniscience, a state of perfect information superiority, prevents surprise. Building on this theoretical extreme, the monograph presents a new definition of surprise, the components of surprise, a visual model of surprise and summarizes planning and execution procedures for deliberate surprise attacks. All of these hypothesis pieces are information superiority based. The monograph does not submit the hypothesis to sufficient testing to claim this to be a theory.

This is a starting point. After rigorous testing and discussion, the hypothesis has the potential to drive changes in doctrine, the education system, training, and simulations. Furthermore, a mature version of this hypothesis may promote adjustments to current staff structures. At the very least, the monograph suggests that the current understanding of surprise can improve. The United States military's undisputed power on the conventional battlefield could force adversaries to use surprise in order to level the playing fields. The U.S. military must understand this principle of war both to counter future enemy actions and to improve its own military operations.

Table of Contents

CHAPTER 1

The Elusive Principle of War

"September 11, 2001-- 08:48 Eastern Time. This just in. You are looking at obviously a very disturbing live shot there. That is the World Trade Center, and [we] have unconfirmed reports this morning that a plane has crashed into one of the towers of the World Trade Center."[1] This CNN transcript, reminds us that in this era of modern technology and telecommunications surprise remains a viable option for militaries of every culture. Later that day, another plane would crash into the World Trade Center and yet another into the Pentagon. The Al Queida terrorist network, in a superbly planned attack, had successfully achieved one the U.S. military's own principles of war, surprise. Surprise still has immense military value and U.S. military planners must know how to achieve surprise on the battlefield.

How do military planners construct plans that achieve surprise? What are the mechanics involved? Military manuals do not provide the answers. Joint and service publications provide definitions of surprise and little else. They do not provide any visual models, theories, tactics, techniques, or surprise planning procedures. The monograph highlights these doctrinal deficiencies points throughout the discussion.

Why are the doctrinal deficiencies concerning surprise of any importance? After all, the United States military has been doing quite well in spite of these deficiencies. So why fix what does not appear to be broken? The reasons are numerous. First, current, updated doctrine provides the basis for education and provides common understanding throughout the force. Second, without well-developed surprise doctrine, it is extremely difficult to plan, synchronize, and execute surprise operations. Third, without well-developed surprise doctrine it is extremely difficult to train for and evaluate surprise operations. Finally and perhaps most importantly, with

[1] CNN Transcript. <http://www.cnn.com/TRANSCRIPTS/0109/11/bn.47.html> (12 November, 2001).

inadequate surprise doctrine, the ability to use surprise as a combat multiplier and the ability to gain the initiative on the battlefield are in jeopardy. Surprise has the potential to achieve military results that far exceed current levels, but without adequate surprise doctrine, the opportunity might be lost. This is a fixable problem.

One way to approach the problem is from the information superiority point of view. Is it possible to construct a hypothesis that explains surprise, one the oldest principles of war, using current doctrinal concept of information superiority? This monograph argues that it is indeed possible to construct a hypothesis using this approach and that the concepts of surprise and information superiority are directly related. This may seem like a formal way to state the obvious, but this relationship extends farther than expected.

This relationship between surprise and information superiority provides the basis for this hypothesis, the hypothesis can provide the foundation for a theory. The military can then use the theory to update doctrinal publication thus correcting the deficiencies. See Figure 1 below for a graphical depiction of the relationship between information superiority and surprise.

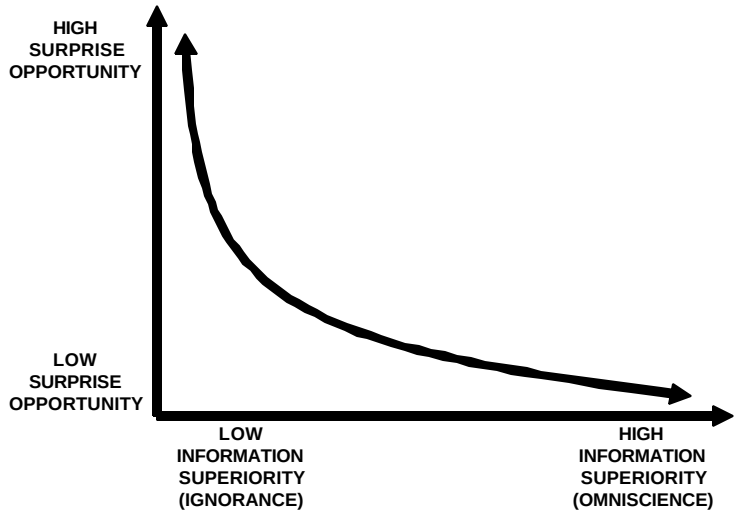

Figure 1. The Axiom

Army Field Manual 3-0, *Operations* states that information superiority "is the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."[2] The theoretical extremes of this definition are no information superiority, ignorance, at one end and omniscience, perfect information superiority at the other. These extremes lead to interesting conclusions. First, it is impossible to surprise a military organization with perfect information superiority. It is theoretically impossible to surprise the organization because it is omniscient. The unit possesses all information, all of the information is correct, and all of the information appears exactly when needed. On the other hand, an organization with no information will always be surprised. It has no relevant information, all of the information they have is incorrect, and all of their information is untimely. These theoretical extremes are the basic assumptions, axioms, used to build the hypothesis.

This monograph uses the Scientific Method to develop the hypothesis (See the top portion of Figure 2 for a summary review of the Scientific Methodology). Chapter 2 and appendix A of the monograph introduce and review the information inputs necessary for hypothesis construction. Chapter 2 explains what appears to be the underlying Clausewitzian theory supporting the current military definition of surprise. In addition, the chapter highlights the key works used to develop this hypothesis. To supplement chapter 2, appendix A provides a complete historical review of surprise theory from a variety of different authors. The historical review introduces surprise theories from a variety of different authors. Chapter 3 constructs the surprise hypothesis in accordance with the hypothesis creation criteria found at the end of this chapter. This chapter provides the new surprise definition, components of surprise, and the visual surprise model. Appendix B supplements Chapter 3. Appendix B contains the data tables, in depth discussions,

[2] US Department of Defense, Field Manual 3-0, *Operations* (Washington, DC: HQs, Department of the Army, June 2001), 11-2.

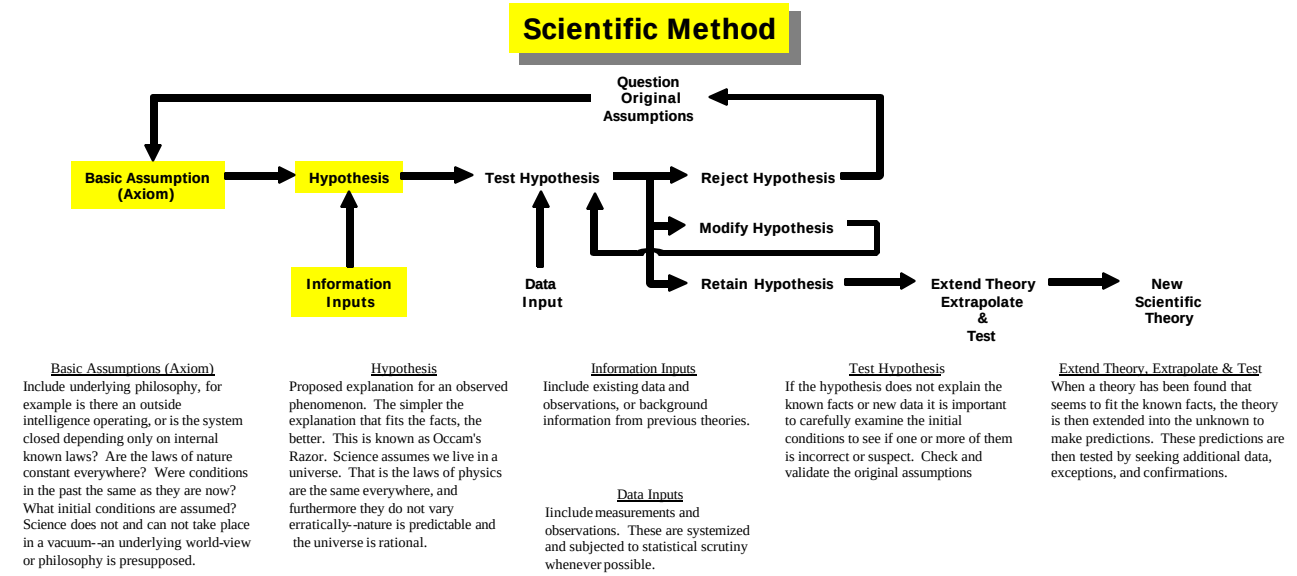

Figure 2. Methodology and Structure

Source: The Scientific Method portion of this figure comes from: Lambert Dolphin, "Steps in the Scientific Method." <http://www.ldolphin.org/SciMeth2.html> (12 October, 2002).

and logic details used during hypothesis construction. Chapter 4 explains surprise from the attacker's point of view and provides effects based tactics, techniques, and procedures that an attacker can use to execute a deliberate surprise attack. Chapter 5 explains surprise from a defender's point of view and explains the effects of surprise on the defender's systems.

This monograph constructs a surprise hypothesis but does not test the hypothesis. Testing of the new hypothesis is beyond the scope of the monograph. This means that at the end of the monograph, the military will have a well-developed hypothesis prepared for testing. This is the first step toward correcting the doctrinal gaps mentioned above. The next step in the Scientific Method should be to submit this hypothesis to historical case study analysis and argument in order to determine if the military should retain, modify, or reject the hypothesis.

To create a successful hypothesis, the monograph must produce a hypothesis that meets the following criteria. The hypothesis must:

Table 1. Hypothesis Creation Criteria	
1	Produce a definition that is clear, concise, and usable throughout the U.S. military community (all services)
2	Determine and describe the components of surprise
3	Produce a visual model depicting the relationship among the definition of surprise and the components of surprise
4	Provide a tactic, technique, procedure, or methodology that an attacker could use to incorporate into the military planning process in order to achieve surprise
5	Provide a way to correct the theoretical and doctrinal deficiencies using existing military resources and force structures
6	Be politically supportable and consistent with the laws of war
7	Be consistent with existing doctrine, thought, and experience

The military profession readily acknowledges that surprise is an important piece of war. However, doctrine does not teach or explain this principle of war very well. Officers and soldiers alike have experienced the benefits of surprise in military operations, but few know the mechanics needed to plan and attain this principle of war. An updated surprise hypothesis could help fix this information gap.

CHAPTER 2

Information Inputs

Chapter 2 accomplishes three major tasks. First, the chapter introduces what appears to be the Clausewitzian theory supporting the current military definition of surprise. Second, the chapter introduces the information inputs (sub-divided into data groups) used to construct the hypothesis. This short historical review highlights some of the key theoretical surprise concepts. Appendix A provides an in depth literature review to supplement Chapter 2. Figure 3 found on the following page, chronologically depicts all of the authors reviewed for this study. Finally, Chapter 3 and appendix A highlight the trends, patterns and gaps in surprise theory found throughout the ages.

Data Group 1: Military Theorists

Secrecy and speed are two constant surprise themes in military theory. Throughout the ages, the names have changed, but the underlying thoughts remain. To surprise the defender, the attacker must keep his plans secret, think faster than the defender, deploy his forces faster than the enemy can react and employ his forces faster than the enemy can react. Works from Clausewitz and Lieutenant Colonel Robert R. Leonhard highlight this point.

Clausewitz understood the importance of surprise. However, he did not support expending a great deal of time and the resources chasing after it. During his era, it was very difficult to surprise anyone while mobilizing, deploying, and employing hundreds of thousands of soldiers. Phrases like "means to gain superiority" and "root of all operations" dot his surprise chapter in *On War.*[3] Clausewitz also recognized that the effects of surprise were predominantly psychological. Confusion, lowering of morale, poor decision-making, and loss of cohesion within the ranks are

[3] Carl Von Clausewitz, *On War,* Ed. and trans. by Sir Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 198.

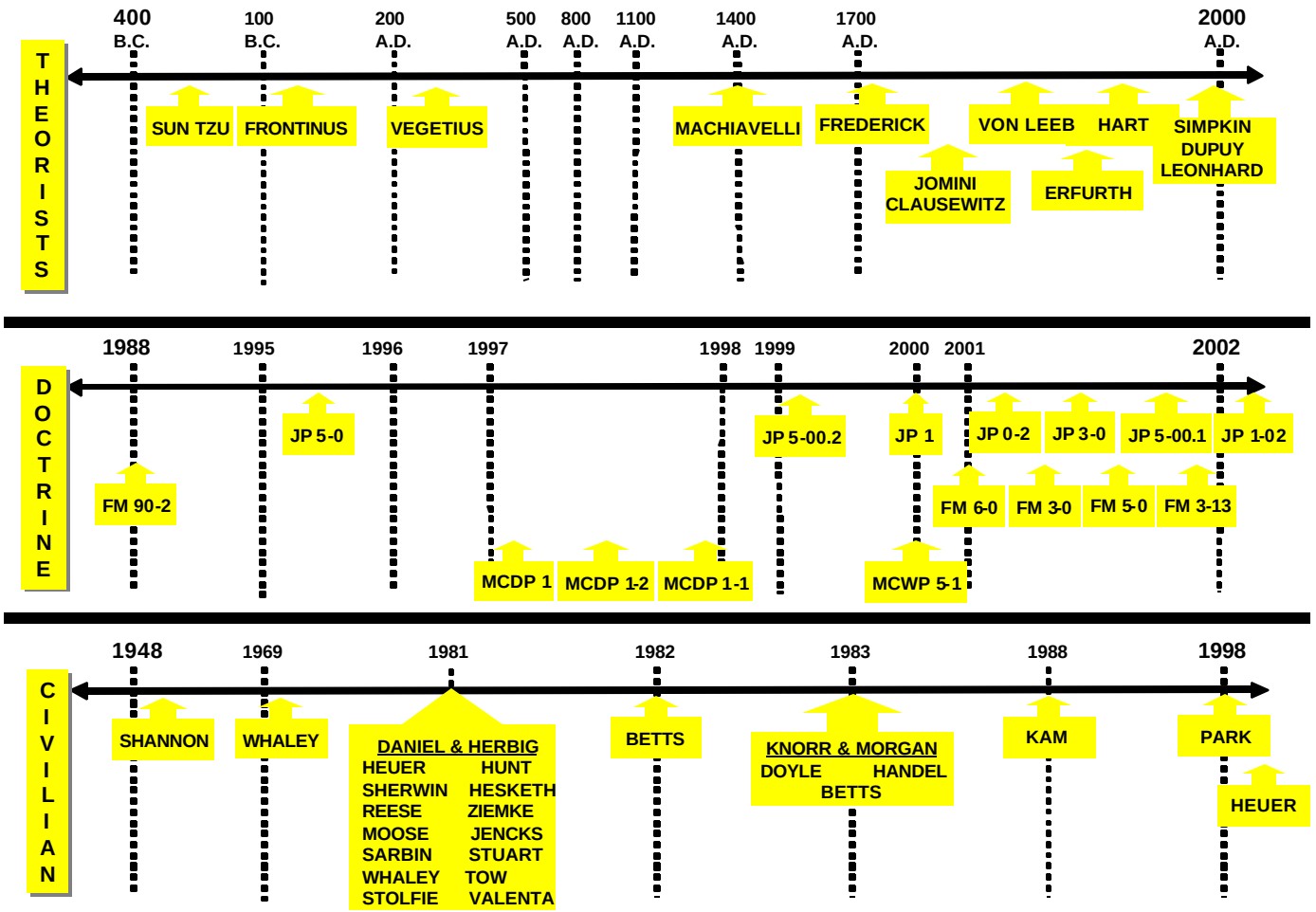

Figure 3. Literature Review

some examples. Additionally, he believed that "The two factors that produce surprise are secrecy and speed."[4] This is the first attempt by anyone to list the components of surprise. He continues his discussion with the components of surprise, "Major success in a surprise action therefore does not depend on the energy, forcefulness, and resolution of the commander."[5] Finally, the great theorist leaves a few rules of thumb:

Table 2. Clausewitz Surprise Maxims	
1	The more friction the harder it is to attain surprise
2	The more time available, the harder it is to attain surprise
3	The greater the ease of achieving surprise, the less its effectiveness
4	Attaining surprise is easier the closer you are to the tactical level of war
5	The less you can impose your will, the less likely you will be to attain surprise
6	It is easier to attain surprise the more offensive your operations

While apparently superior ideas, Clausewitz did not have the opportunity to revisit this chapter prior to his death. Sadly, he leaves his concepts unexplained. The next author Lieutenant Colonel Robert R. Leonhard provides the most recent theoretical thoughts about surprise.

Leonhard begins his discussion on surprise with this quotation: "Yet, for all the attention that we pay to the concept of surprise, there is lacking a thorough conceptual dissection. What is it that composes surprise; what are the theoretical foundations of this most powerful weapon of war? In short, what is the anatomy of surprise?"[6] Leonhard recognized and attempted to address the exact same problems that this monograph attempts to correct.

Leonhard bases his theory on the following axiom: "*military forces are perpetually unready for combat*."[7] In short, this means that if a defender is always 100 percent ready to fight, an attacker could never surprise it. Of course, a military unit can never maintain a combat posture at 100 percent,

[4] Ibid.
[5] Ibid., 200.
[6] Robert R. Leonhard, *Fighting by Minutes, Time and the Art of War* (Westport, CT: Praeger Publishers, 1994), 135.
[7] Ibid., 135.

troops have to eat, troops have to sleep and vehicles break down. Leonhard defines surprise with the following: "Surprise is a condition in which a military force is contacted while in a relative state of unreadiness."[8] He continues his discussion by saying that surprise is temporal and "results (either accidentally or by design) from a failed time-distance calculation on the part of the surprised force."[9] His components of surprise are detection and contact (See Figure 2-2 below).

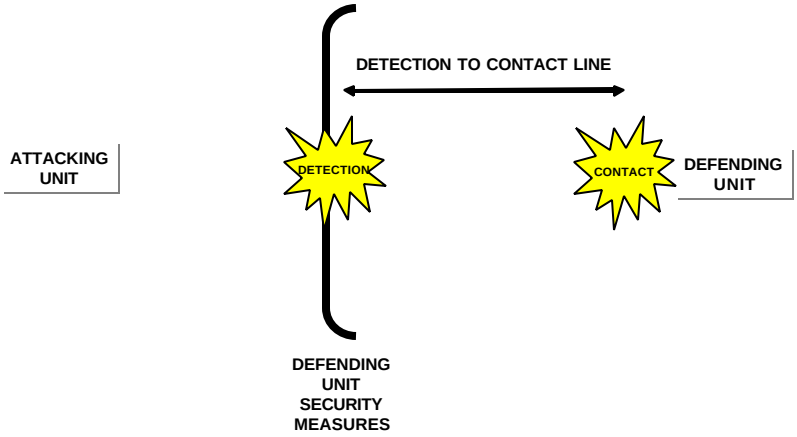

Figure 4. Leonhard Surprise Model

Detection occurs when the defending force security measures or security forces identify an approaching enemy threat. The identification of this threat awakens the defending unit from its state of unreadiness. Contact results when the attacking force meets the defending force. If the attacking unit can make contact with the defending force faster than the defending force can awaken from its perpetual unreadiness, then the defending unit is surprised. Therefore, a desire to delay detection and

[8] Ibid, 140.
[9] Ibid.

a desire to hasten contact once detection occurs are the two components of surprise for Leonhard.[10] The more an attacker can shorten the detection to contact line, the more likely he is able to catch the defending force in a state of unreadiness. Thus, the more likely the attacking force will surprise the defending force.

Leonhard's ideas appear to be an updated version of the same two components Clausewitz discussed, secrecy and speed. Using Clausewitz' words in Leonhard's model would sound something like: Keep your plans and movements secret for as long as possible. Once these plans and movements are discovered move at maximum possible speed to engage the enemy.

In his second book, *The Principles of War for the Information Age*, Leonhard updates his original concept of surprise. The general goal in Leonhard's surprise model remains constant. The attacker wants to delay detection and once detected, contact the enemy before he can recover from his state of unreadiness. He adds a revised definition: "Surprise is a battlefield condition that results from the interaction of two components: perpetual unreadiness and time."[11] In summary, the attacker exploits the defender's perpetual unreadiness by delaying detection and hastening contact once the defender's security measures detect the attacker. This process is dependent upon time. It is a time measurement of whether you can contact the enemy before he can awaken from his unreadiness. Again, this updated version of the theory remains very similar to the concepts of secrecy and speed originating with Clausewitz.

History has not produced a great deal of theoretical thought to provide a basis for doctrine. This may be why military definitions of surprise are confusing and sometimes contradictory. Furthermore, it appears that the military experiences with surprise seem to be beyond explanation or recording. While militaries of every culture have always considered surprise a vital aspect of war, the analysis of surprise does not seem to have been a priority in the Western military culture.

---

[10] Ibid.
[11] Robert R. Leonhard, *The Principles of War for the Information Age* (Novato, CA: Presidio Press, Inc., 1998), 183.

Data Group 2: Doctrine

Field Manual 3-0 *Operations* and FM 3-13, *Information Operations: Doctrine; Tactics, Techniques, and Procedures (DRAG Draft)*, FMs vital to the construction of this hypothesis.

FM 3-0 makes a bold break from the normal trends in surprise theory. This manual suggests that a linkage exists between surprise and information superiority. Taking an attacker's point of view, FM 3-0 says that "Estimating the enemy commander's intent and denying him the ability to gain thorough and timely situational understanding is necessary to achieve surprise." FM 3-0 also mentions that military formations can avoid surprise by continuously updating their intelligence.[12] FM 3-0 makes a final point critical to the hypothesis:

> Gaps are elements of information commanders need to achieve situational understanding but do not have. Ideally, analysis identifies gaps and translates them into specified requirements. To fill gaps, commanders and staffs make assumptions, clearly identifying them as such. There may be circumstances when commanders and staffs fail to identify a gap. Such circumstances are especially dangerous, particularly when facing an asymmetric threat. The commander not only does not have a piece of relevant information, but also does no know he needs it. This situation may result in the commander being surprised. Commanders and staffs remain adaptive and examine circumstances as they are, rather than fitting circumstances into preconceived notions.[13]

This is a very important quotation, central to this monograph. The quotation highlights the importance of information gaps. When a military organization has information gaps, it must fill these gaps with assumptions in order to continue planning. When the organization makes assumptions, its assumptions are subject to many different forms of biases. Chapter 5 covers the linkage among information gaps, assumptions, and biases in more depth.

A second manual critical to hypothesis development is FM 3-13. This manual implements Joint Information Operations doctrine established in Joint Publication (JP) 3-13, *Joint Doctrine for Information Operations*. Additionally, FM 3-13 establishes the doctrine, tactics, techniques, and procedures used for IO. For this study, FM 3-13 along with JP 3-13 will provide the basis for the

[12] US Department of Defense, Field Manual 3-0, *Operations* (Washington, D.C.: HQs, Department of the Army, June 2001), 8-8.
[13] Ibid., 11-12.

construction of surprise operation tactics, techniques, and procedures (TTPs) found in chapter 4. Like IO, the surprise operation TTPs in this hypothesis will follow the targeting methodology, a familiar and comfortable model to most of the Army.

Data Group 3: Civilian Sector

The vast majority of the civilian publication studies concentrate on surprise at the strategic level of war. The studies attempt to uncover strategic level causes of surprise and they provide strategic level solutions to these causes. However, the civilian sector's conclusions and recommendations appear to be quite relevant to the operational and tactical levels of war as well. The studies generally agree that surprise occurs as the result of four factors: informational deficiencies, decision-making deficiencies, organizational deficiencies, or cognitive deficiencies. One recent author Richards J. Heuer Jr. highlights these thoughts very well.

In his book *Psychology of Intelligence Analysis*, Mr. Heuer ties together the concepts of cognitive psychology and intelligence analysis. His basic thesis is that mental information processing pitfalls are part of every human; thus, the pitfalls cannot just disappear. When people screen information, sort through information, evaluate information, hypothesize, and make assumptions, they make errors. These errors are predictable and they are exploitable. When people must make judgments in atmospheres of ambiguous information, the normal environment for a defender during a surprise attack, they are susceptible to hypothesizing and assumption making because they do not have the necessary relevant information. These hypotheses and assumptions are susceptible to biases, and these biases are susceptible to exploitation. The defender has no choice. He is under extreme time pressure to figure out what the attacker is doing so he can produce an effective countermeasure.[14] Again, chapter 5 will add more depth to this discussion.

[14] Richards J. Heuer Jr., *Psychology of Intelligence Analysis*. <http://www.odci.gov/csi/books/19104/index.html> (23 December, 2002).

Summary

It appears that the world is generally only interested in surprise following catastrophic events resulting from surprise. Surprise studies surged following the Japanese attack on Pearl Harbor, the Arab-Israeli wars, and U.S.-Soviet tensions during the early 1980s. Following this same pattern, surprise study will again peak due to the events of 11 September.

The Military tends to think of surprise in terms of secrecy, speed, or some derivative of the two. The civilian sector zeros in on intelligence, surveillance, reconnaissance (ISR), and information management failures. All information input groups agree that information operations, especially deception, play a prominent role in any surprise operation. No single work from any of the information input groups adequately addresses the criteria set forth in chapter 1.

Based on the lack of surprise information in doctrine, it appears that the U.S. military has not historically placed a high value on surprise. The reasons may be cultural, historical, or political. Nevertheless, these reasons do not justify a lack of doctrine and theory for surprise. Consciously, choosing not to use surprise is quite different from not knowing how to use surprise. When the U.S. decides to plan and conduct surprise operations, as it has many times in the past, the military does quite well. Unfortunately, U.S. military manuals have not done well passing on the knowledge gained from these experiences. There is much more to surprise than just secrecy and speed...much more.

CHAPTER 3

An Alternate View of Surprise

Chapter 1 introduced the axiom supporting this monograph. The axiom is this: perfect information superiority (IS) equals no surprise and no IS equals always surprised. This thought is the basic assumption underlying the hypothesis. This chapter, using the information inputs from chapter 2 and appendix A, expands the axiom to accomplish three additional tasks. First, the chapter develops an updated definition of surprise. This definition will tie surprise to IS. Second, analysis clears away all of the literary chaff to isolate the constituent components of surprise. These constituent components are the conditions that must be present for surprise to occur. Finally, the chapter offers a visual surprise model. The model visually depicts the monograph's key concepts and the major systems involved with surprise. With the axiom, definition, components, and visual model, the hypothesis is well on its way meeting the hypothesis creation criteria established in chapter 1.

One point requires clarification prior to the definition development. Any discussion about surprise has two perspectives, the attacker's perspective and the defender's perspective. The perspectives are different. This is not an earth-shattering idea and seems rather obvious. However, this point is critical to understanding surprise. Any discussion that inadequately addresses one of the perspectives might create confusion. For example, military theorists and military doctrine discuss surprise from the attacker's point of view and offer little information from the defender's perspective. In contrast, the civilian sector focuses much of their effort on the defender and does not offer much for the attacker. A complete hypothesis must address both perspectives. From this point forward, the monograph addresses both perspectives throughout the discussions. Now the construction of an updated surprise definition can proceed.

Basic Definition of Surprise

Historically, surprise has proved very difficult to define. Authors have used every conceivable way to develop their surprise definitions. Sometimes the authors have even used combinations of definition development methods. These leads multiple definition development methodologies lead to even more confusion. Current doctrine falls into this category. While it is challenging to develop an appropriate definition of surprise, it is not impossible. The new definition must state the essence of surprise,[15] must be clear and concise, has to be appropriate for all military services, has to be flexible enough to keep pace with changes in the spectrum of conflict, and must be appropriate to both the attacker's and defender's point of view. Furthermore, the updated definition must use current IS doctrinal terminology. This self-imposed constraint will ensure the resulting definition is compatible with current doctrine. This constraint also preserves the logic link between the axiom and the definition.

The definition creation followed a two-step process. The first step collected all of the available surprise definitions from each of the data groups. The second step screened the definitions to eliminate all synonyms, methods to achieve surprise, purposes of surprise, components of surprise, types of surprise, and conditions related to surprise (Appendix B provides a detailed talk through of the definition screening process). The screening process ensured a single definition development method that in turn ensured clarity in the new definition.

[15] The monograph has at least five different ways to form the new definition. The generally accepted methods are definition by synonym, by example, by stipulative method, by providing the necessary and sufficient conditions that must be met, or by stating the essence of that which is to be defined. This hypothesis uses the "essence" method to define surprise. The other methods can result in confusing definitions. For example, synonym definitions beg a further definition of the synonym being used. Example definitions sometimes add additional complexity that requires additional explanation. Stipulative and conditional definitions are probably too restrictive and inflexible for military doctrine. Essence definitions are clear and concise. An example of an essence definition is to define man as a rational animal. Moreover, the "essence" definition is flexible enough to accommodate change but not so flexible that it useless. The essence definition is the type of definition that appears to work very well for this situation. For more information about definition creation see: Sylvan Barnett and Hugo Bedau, eds., *Critical Thinking, Reading, and Writing, a Brief Guide to Argument* (New York, New York: Bedford/St. Martin's, 1999), 56.

The following phrases remained after the screening process: "unexpected, a military act, violations of the victim's expectations and assumptions, an effect caused through being unexpected". This is very little to work with, but it is sufficient. After combining and rearranging these phrases, the following is the basic definition of military surprise: *Surprise is the effects of unexpected military actions.*

A few more discussion points remain. First, "expectations and assumptions" are conspicuously absent from the basic definition. This is because expectations and assumptions are defender specific. They are not normally a concern for the attacker. The definition must be appropriate for both sides of the coin. Chapter 5 provides more depth to the defender expectation and assumption discussion. Even though this basic definition seems acceptable, it does not meet the self-imposed constraint discussed earlier. The new definition must use IS doctrinal terminology. This is possible. However, the monograph must introduce the surprise components first. The definition discussion continues in the advanced definition section of the chapter following the surprise component discussion, the next topic.

The Components of Surprise

This section attempts to determine the components of surprise from the information inputs provided in chapter 2 and appendix A. A component, by definition, means a constituent or essential part.[16] In other words, a component of surprise is something that must be present for surprise to occur. Some might refer to this, as the necessary and sufficient conditions needed for achieving surprise. This is a very restrictive focus, and it is intentionally restrictive. The hypothesis must impose this constraint to prevent developing a list of hundreds of components, something similar to the current military definitions of surprise. A lengthy list of surprise components would only add to the confusion.

[16] Merriam-Webster Online. < http://www.m-w.com/> (11 October 2002).

The screening methodology for surprise components is the same as that used for definition creation: step one collected all available evidence, and step two screened the list of potential components. Since the available component list was so diverse, the analysis process screened each component separately using a detailed systemic process (See appendix B for the detailed component screening process). In addition, the analysis renamed some of the existing components during the screening process to match current doctrine terminology. The results of this process did support and mesh with the hypothesis axiom.

The research concludes with the following: *surprise is a function of attacker exploitation, defender ISR system deficiencies, and defender IM system deficiencies.* These three components are constituent to surprise (See appendix C for a review of IS, ISR, IM and IO to assist with all of the definitions required to understand these relationships). This appears to be solid logic: defender ISR and IM system deficiencies result in defender information gaps and should an attacker exploit these defender information gaps he will surprise the defender. A formula might look something like the following:

SURPRISE COMPONENT EQUATIONS

(1) Surprise = Attacker Exploitation + (Defender ISR deficiencies + Defender IM deficiencies)

(2) (Defender ISR deficiencies + Defender IM deficiencies) = Defender Information Gaps

Formulas (1) and (2) can be re-written as:

(3) Surprise = Attacker Exploitation + Defender Information Gaps

Advanced Definition of Surprise

Now that the analysis has isolated the components of surprise, the hypothesis construction further the basic definition to an advanced definition. The definition end-state requires a definition expressed with IS doctrinal terminology. The final definition of surprise results from a combination of the basic definition and the surprise component formulas. The below explanation further describes the relationship:

1. Basic Definition: Surprise is the effects of unexpected military actions.
2. Combined with the Surprise Component Equations:
   - Attacker Exploitation + (Defender ISR deficiencies + Defender IM deficiencies)

- Where (Defender ISR deficiencies + Defender IM Deficiencies) = Defender Info Gaps

3. Yields the Advanced Definition: *Surprise is the effects of attacker exploitation of defender information gaps.*

The link between the basic definition and the advanced definition is the word unexpected. For the defender, unexpected events occur when he does not have the appropriate relevant information. By doctrinal definition, when the defender does not have relevant information he has an information gap. Furthermore, unexploited defender information gaps are only ignorance. Once the attacker exploits the information gaps, however, he attains the effects of surprise. Therefore, attacker exploitation must also be part of the definition. Visual model creation is the next step of the process.

The Model

Surprise is a system composed of several other systems. It is impossible to model all of the interactions involved with surprise. Therefore, this model only depicts the major systems comprising surprise. Time compounds this challenge. Surprise and all of the interactions among the systems comprising surprise are temporal. Time is a very definite element to all surprise operations. All of these challenges aside, Figure 5, shown on the next page, depicts a visual attempt to capture surprise.

The model has several pieces, some of which the discussion already introduced. The top of the model depicts the attacker's major systems involved with surprise: Decision Maker System (OODA Loop), ISR System (Intelligence Cycle), Offensive Information Operation planning and execution system (D3A), and the Operations Process (maneuver/countermeasure system). The bottom of the model shows the defender's systems. The model splits the attacker and defender sections with a timeline and a box titled Effects of Surprise. Chapter 4 covers the effects of surprise. Finally, the lower left quadrant of the model has two graphs. These graphs show the relationship among information gaps, surprise opportunities, and the passage of time. The model only depicts the systems most relevant to the monograph.

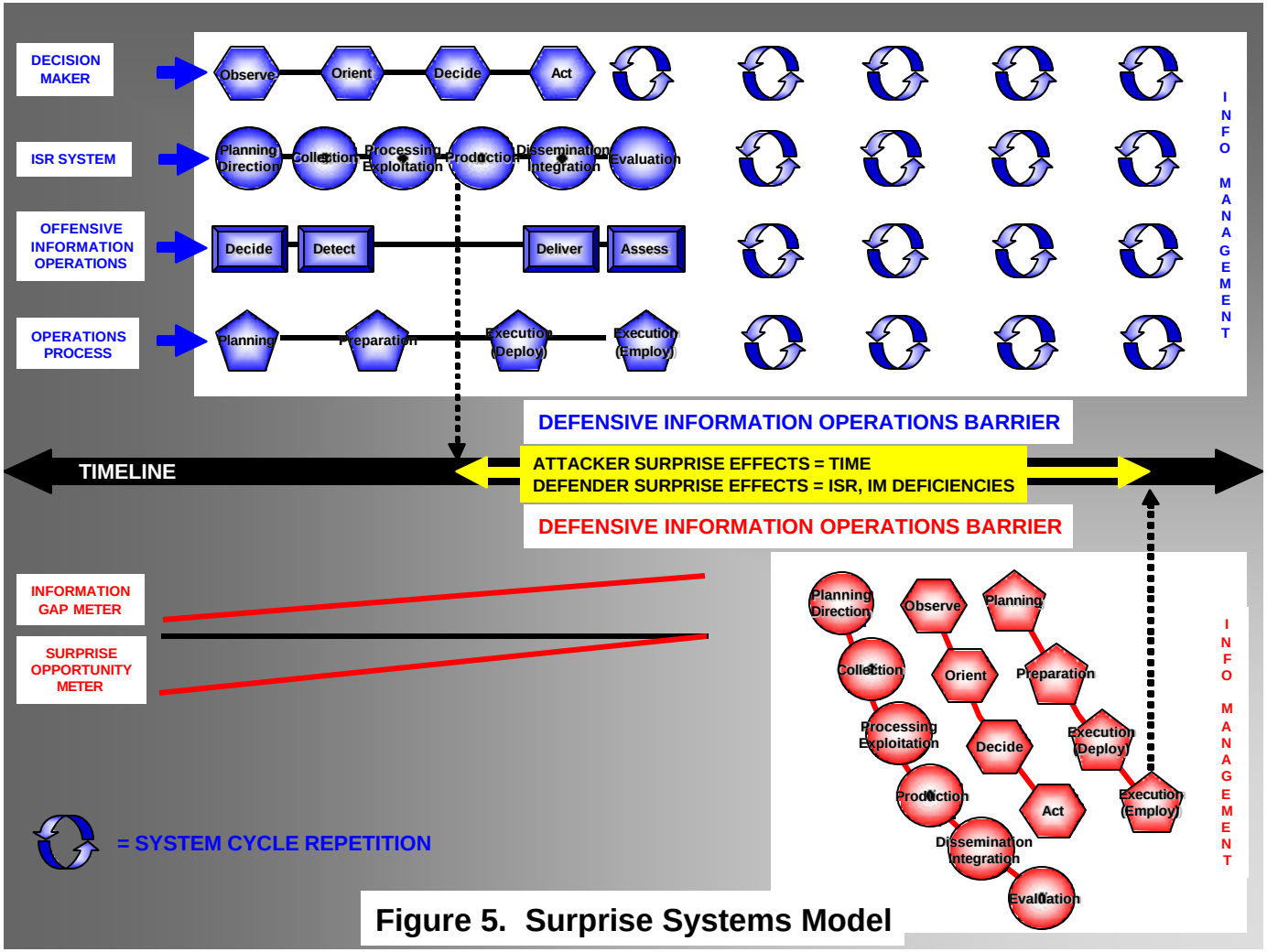

Figure 5. Surprise Systems Model

Summary

Chapter 3 began with the underlying axiom to the hypothesis: it is impossible to surprise military organizations with perfect Information Superiority. From that starting point, using the information inputs from chapter 2 and appendix A, the analysis produced a definition of surprise, isolated the components of surprise, and presented a visual model of surprise. Essentially, the logic boils down to the following: If an attacker, whether knowingly or unknowingly, exploits a defender information gap, he will surprise the defender and gain the initiative on the battlefield. Figure 6 on the following page graphically attempts to clarify the logic further. So far, the monograph explained what surprise is and why surprise occurs. The next step is to determine how the attacker plans and executes deliberate surprise operations, another of the hypothesis creation criteria from chapter 1. This is the topic of the next chapter.

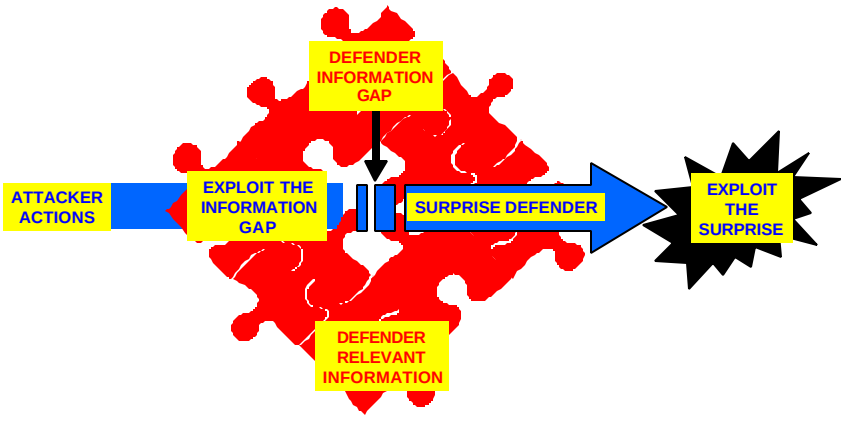

Figure 6. Surprise Summary Graphic

CHAPTER 4

Attacker Exploitation, the First Component of Surprise

One of the links between theory and application are tactics, techniques, and procedures (TTPs). Current doctrine does not have TTPs that explain how to move from surprise theory to application. There is a definition of surprise and generalized statements sprinkled throughout various manuals. That is all there is in doctrine. Chapter 4 attempts to address that deficiency for this monograph's hypothesis. Chapter 4 continues to expand the hypothesis by presenting planning and execution TTPs that an attacker can use to create and exploit surprise in deliberate surprise attack operations. The TTPs are effects based and is a close replication of the Fire Support planning model. The TTPs work using the decide, detect, deliver, assess (D3A) methodology within the targeting process environment. While many other TTPs may work well for surprise operations, these TTPs have already proven to work well with Information Operations (IO), an important feature explained later in the chapter.

Essentially, the deliberate surprise attack has two phases of execution.[17] The first phase sets the conditions, and the second phase exploits these conditions. In the first phase, offensive information operations attack the enemy systems to achieve the effects of surprise. This is the shaping operation. Next, the decisive operation, normally the maneuver forces, exploits the effects of surprise. This concept is simple enough, but requires a more detailed look.

This TTP has four parts: task, purpose, method, and effects measurements. Each of the TTP parts grew from the same two-step data analysis methodology used in chapter 3. The first step collected all of the relevant data. The second step screened all of the collected raw data to produce the screened data and final observations. The Research and analysis produced some very interesting results.

Task

The surprise attack task has three subcomponents: Targeting Objective, Formation, and Function and/or Capability. All three subcomponents must be present in the task statement. This task statement division adds a greater specificity to the task, instills discipline on the task creation process, and provides the appropriate catalysts needed to start the targeting process. All parts are necessary for the task statement and the TTP.

Targeting Objective

The targeting objective is a description, normally a one-word description, of the conditions that will produce the effects desired. With surprise, the targeting objectives must describe the conditions that produce the effects of surprise. In this hypothesis, the conditions that create surprise are decreased defender information superiority through decreased defender ISR and IM system efficiency. Using this logic, the attacker should direct the surprise targeting objectives to the defender ISR and IM systems.

The doctrine data group supported this logic while the civilian sector and theorist data groups neither confirmed nor denied the logic. This is not particularly surprising. The targeting concept works for modern-day operations using current doctrine. It may or may not work with historical evidence in the historical context. Therefore, the answers will have to come solely from current doctrine. More specifically, the hypothesis uses IO targeting objectives because by doctrine, definition, description, and design, IO manipulate attacker and defender IS. This is a perfect fit.

JP 3-13.1 makes an early attempt to describe the targeting objectives associated with IO. The manual lists deny, influence, degrade, and destroy as the primary targeting objectives.[18] However, research and analysis concentrated on FM 3-13 because this manual provides the most

---

[17] The phrase "deliberate surprise attack" differentiates from an operation that accidentally surprises the defender.

[18] US Department of Defense, Joint Publication 3-13.1, *Joint Doctrine for Command and Control Warfare (C2W)* (Washington, D.C.: Joint Chiefs of Staff, 7 February 1996), v.

recent material concerning IO targeting objectives. FM 3-13 lists the following IO targeting objectives: deceive, degrade, deny, destroy, disrupt, exploit, and influence.[19]

These targeting objectives are fine as they are. They do not require any further screening or analysis. To create the conditions necessary for surprise, the attacker must decrease the defender IS by creating information gaps. To create the information gaps, he must increase the defender's ISR and IM deficiencies. To increase the defender's ISR and IM deficiencies, the attacker directs the IO targeting objectives at defender ISR and IM targets. The next subcomponent, formation, further defines the defender's ISR and IM target sets.

Formation

This section develops target sets for a deliberate surprise attack. These target sets are where the attacker directs his targeting objectives and what he will attack with his offensive IO. Most of the authors recognized that the attacker should direct espionage and deception activities to the defender's ISR system and defender's decision makers. Additionally, Richard Betts, KlausKnorr, Patrick Morgan, and Ephraim Kam highlight the importance of focusing efforts toward the defender's ISR system, IM system, and decision maker. However, none of the authors offered target lists. Unfortunately, a target list is exactly what the TTP needs. Therefore, JP 3-13.1 and FM 3-13 will again have to provide the answers. Luckily, these two manuals hit another home run.

The target lists found in JP 3-13.1 and FM 3-13 are a perfect fit for surprise operations. Both manuals suggest that the attacker target the following defender systems: defensive IO, ISR, IM, Decision Making, and countermeasure. This target list matches the hypothesis well. To create information gaps, the attacker must break through the defender's defensive IO system (if one exists) and attack the defender's ISR, and IM systems. Additionally, the attacker must attack the links between these systems. Figure 7 graphically depicts the target sets.

[19] While most of us are very familiar with these, Appendix B lists a complete description and definition for

There is one final note. It is not necessary to attack the defender's decision-making system and countermeasure force to achieve and exploit surprise. However, it is clearly prudent planning to consider doing so in order to prevent any possible defender decisions and countermeasures. Attacking the additional target sets is an added insurance policy. From here forward, the defender's decision-making system and countermeasure force are valid surprise target sets.

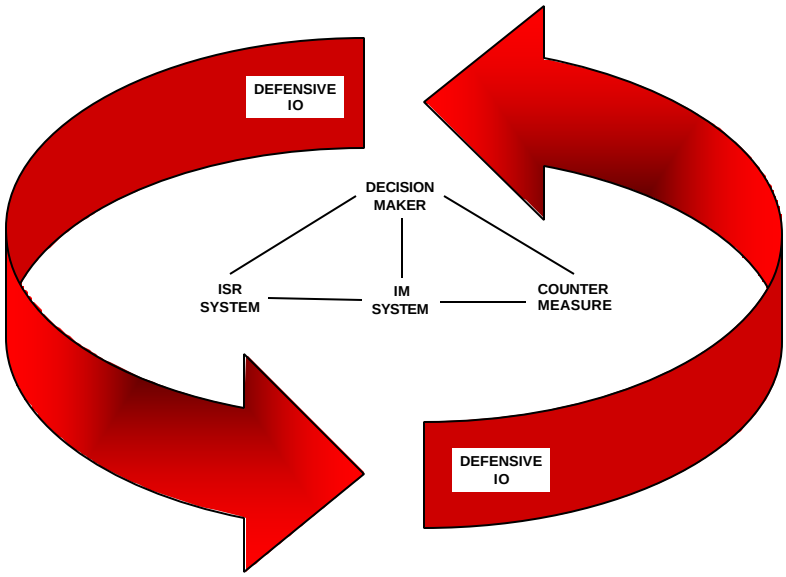

Figure 7. Surprise Target Sets

Function/Capability

Thus far, the TTP has described the targeting objectives IO must achieve (objective) in order to attain surprise. Furthermore, the discussion has highlighted the targets the attacker must attack (formation) to achieve surprise. This is not enough. The TTP must also describe the specific function or capability of the target the attack attempts to affect. The TTP terms this the function. In a deliberate surprise attack, the attacker attempts to decrease the efficiencies of the defender's

---

each.

ISR and IM systems. These system efficiencies are the functions and capabilities he tries to affect. However, this description must be more specific.

The monograph research produced an abundance of material for this topic (See appendix B, Table B7 for the raw function data). Each of the data groups addressed each of the target sets adequately. The screening and analysis needed only to rearrange the information into a useable form. Therefore, the screening process reorganized the data according to the target sets developed earlier. Table 3 shows the results of the reorganization effort.

Table 3. Screened Function Data

Defender Defensive IO System	Ability to defeat attacker Offensive Information Operations
Defender Decision Making System	Ability to observe
	Ability to orient
	Ability to decide
	Ability to act
Defender ISR System	Ability to plan ISR system
	Ability to direct ISR system
	Ability to collect information
	Ability to process information
	Ability to exploit information
	Ability to produce relevant information
	Ability to disseminate relevant information
Defender IM system	Ability to pass relevant information among the systems
	Ability to integrate relevant information among the defenders' systems
Defender Countermeasure System	Ability to deploy countermeasures
	Ability to employ countermeasures

Table 3 describes the deliberate surprise attack function or capability sufficiently for planning. The function or capability subcomponent is the last piece needed to produce a complete task statement. The following examples tie all three of the subcomponents together into complete task statements for deliberate surprise attacks: (1) Attacker electronic warfare agencies disrupt defender XX Corps ISR system abilities to collect information, and (2) Attacker assets destroy (physical destruction IO) defender XX Corps C2 node decision-making ability.

While these task statements are enough to start the targeting process, they are insufficient for planning. Every military operation must have a purpose. Deliberate surprise attacks are no different.

Purpose

The attacker must explain why he is conducting his deliberate surprise attack. Additionally, he must explain how or what the deliberate surprise attack contributes to maneuver operations. Like other shaping and enabling operations, the attacker must nest his deliberate surprise attack with maneuver operations. This way the attacker can ensure that he is prepared to exploit the effects of surprise. The attacker can do all of this with a purpose statement.

Anyone who has read a military manual has heard that surprise is a combat multiplier. The statement has been in military surprise definitions since militaries first started making manuals. What exactly is a combat multiplier? What does it mean? Military manuals do not explain this point very well. Research, however, explained exactly what being a combat multiplier means and in the process, explained what a purpose statement for a deliberate surprise attack should look like.

Surprise is a shaping and sometimes an enabling operation. It can help a maneuver force attain four other principles of war: economy of force, maneuver, mass, and offensive. This is what phrase "combat multiplier" means, and this is a description of how surprise can contribute to maneuver operations. Surprise can allow the decisive operation achieve economy of force, allow the decisive operation to maneuver, allow the decisive operation to mass, and or allow the decisive operation to achieve and maintain the offensive. These are great purpose statements and do not require further analysis.

This ends the discussion of the purpose statement for deliberate surprise attacks. The information inputs proved very helpful. With a task and purpose in hand, the analysis can proceed with the "method" portion of the TTP.

Method

The fire support model that this surprise model replicates expresses its methodology in the following format: priority, allocation, and restrictions. In the fire support model, "priority" delineates the maneuver unit that has priority of fire support. "Allocation" explains the asset allocations throughout the battlefield. Finally, "restrictions" explains the restraints and constraints imposed on the use of fire support assets. This planning format works well for tactical level fire support planning, but may or may not work well for deliberate surprise operations. The monograph does not explore the issue any further. However, what the monograph does examine is the methodology used to produce the priority, allocation, and restrictions format, that beingthe decide, detect, deliver, assess (D3A) methodology. The fire support and IO communities use the D3A methodology within the targeting process to plan and synchronize their effects based operations. Since this hypothesis proposes using IO to create the conditions necessary to attain and exploit surprise, it seems appropriate that the hypothesis should use the current IO methodology.

So how does the attacker attain the conditions necessary for surprise? How does the attacker create the information gaps discussed in the monograph? What tools does he use? Doctrine does provide the answers to these questions without realizing it. It is obvious, so obvious that current military theories and doctrine may have overlooked the connection. The attacker must use offensive IO to increase the defender ISR and IM system deficiencies. This will create the information gaps the attacker seeks. Once he creates these gaps, the attacker can exploit these gaps, surprise the defender, and exploit the surprise to gain the initiative on the battlefield.

Offensive IO planners have already developed their ownTTPs in FM 3-13. These detailed TTPs are entirely adequate and compatible with deliberate surprise attack planning and execution. This discussion will not review them. Instead, the discussion will highlight some of the peculiarities relevant to surprise operations using the D3A methodology as a discussion structure (Appendix C provides a review of the D3A and Targeting Process).

Decide

A major attacker decision during the decide phase is to determine whether he wants to attack existing defender information gaps or whether he wants to create defender information gaps and exploit those. Realistically, it is unlikely that the attacker will know the defender's existing information gaps ahead of time to any degree of certainty. However, in both approaches, the attacker should use some form of Target Value Analysis (TVA) to determine the High Value Targets (HVTs). In a deliberate surprise attack, the HVTs should originate from one of the defender's target sets discussed earlier: defensive IO system, ISR system, IM system, decision-making system, countermeasure system, and or the links among all of these defender systems.

A second major task, like in all targeting operations, is to locate the target. The targets include the components, nodes, and links for all of these defender systems. If the attacker cannot determine some of the locations, he can template the suspected locations and then assign assets to confirm or deny the locations using his own systems. This process is no different from what the current methods of dealing with unknown HVT locations.

Finally, the attacker must establish his feedback loops. The purpose of the feedback loop is to help the attacker determine if his offensive IO has been effective. The attacker has innumerable options for feedback loops. He has his choice of any of the normal ISR systems (IMINT, HUMINT, SIGINT, MASINT, OSINT, or TECHINT), maneuver formations, or combat support formations (such as forward observers) to provide this service. If the attacker's operation relies heavily on surprise for success (forcible entry operations might be a good example of such a case), this feedback loop is critical.

Once the attacker has decided what he wants to attack and where he wants to attack, he can incorporate the deliberate surprise attack HVTs into the High Payoff Target List (HPTL), the Target Selection Standards (TSS), and the Attack Guidance Matrix (AGM) via the normal Targeting Process procedures. These products are the inputs for the detect phase.

Detect

The first task for the attacker is to confirm and or deny the locations of his list of suspected surprise targets. Additionally, he should ensure that his feedback loops are fully mission capable. Other tasks include updating the surprise attack HPTL and AGM. Finally, the attacker might consider testing the defender's systems. More specifically, this means testing the efficiencies of the defender's systems. While this is not necessary and time rarely allows for this, it should be a consideration. The attacker can test the defender's reaction efficiency by conducting feints, demonstrations, show of force operations, and training operations at or near the intended location of the actual operation. While it might seem counterintuitive for the attacker to practice his surprise attack ahead of time in full view of the enemy, this method can and has proved useful. The U.S. used this approach prior to Operation Just Cause to test reactions and reaction times of the Panamanian forces. The estimated defender reaction time provides a general estimate of the defender ISR, IM, decision-making, and countermeasure efficiencies. The chapter discusses this concept in the "effects measurement" section.

Deliver

This is the attacker's Offensive IO execution phase. Once the offensive IO begin, the defender's information superiority will begin to decline as the attacker increases the defender's information gaps. Once the defender's information gaps reach the level the attacker desires, he can attack the information gaps, attain surprise, and exploit surprise. The attacker has numerous options available for delivery. He can physically destroy parts of the defender's systems. He can temporarily degrade parts of the defender systems with electronic warfare. The attacker can also flood the defender's systems with irrelevant information, called distracters. Additionally, he can also reduce the flow of information or manipulate the flow of information so that the defender receives very little, but very wrong information. Only imagination limits the attacker's use of the hundreds of combinations available.

Assess

Although listed as a separate phase, assessment occurs throughout the D3A methodology and targeting process. In this case, the attacker is especially concerned with tracking the status of Offensive IO to determine if he is achieving his targeting objectives. The feedback loop, established earlier in the D3A and targeting processes, provides this information. Secondly, the attacker must continually assess the process to determine the defender's adaptations to the attack. The defender's systems will adapt. No force will tolerate the loss of one of the types of systems that the attacker is attempting to effect. The defender will attempt to adapt to overcome the attacks. Finally and maybe most importantly, the attacker must monitor his offensive IO to track the second and third order effects of his operations. Like the defender's adaptations, second and third order effects will occur. The attacker must anticipate and be capable of reacting to these wanted and unwanted effects.

As mentioned at the beginning of this section, the discussion attempted to highlight some of the methodology considerations peculiar to surprise operations. FM 3-13 provides in-depth, detailed offensive IO TTPs. Effects measurement is the next topic, and this proved to be the most challenging part of the hypothesis development.

Effects Measurement

Effects measurement quantifies successful accomplishment of the mission. These are measures of effectiveness. The attacker uses effects measurement during his assessment process to determine if a re-attack or re-application of effects is necessary. These measurements determine mission success or failure.

Surprise has two perspectives or two sets of effects, the effects from the attacker's point of view and a different set of effects on the defender's side of the equation. On the attacker's side, the effects of surprise can provide the ability to mass, maneuver, seize and or retain the initiative, and conduct economy of force operations. For the defender, surprise produces the negative

effects of shock, paralysis, confusion, poor decision making, lowered moral, conflicting orders, and others. The challenge in this section is to determine a surprise effect measurement compatible with both perspectives.

Surprisingly, this research uncovered several different ways to measure the effects of surprise. Gaming Theory, Communications Theory, and Information Theory are examples that use probability based surprise measurements. Probability methods focus on measuring the probability of occurrence of an event. For example, with this method, the defender would assign probabilities to all of the different attacker's courses of action. The attacker's course of action assigned the highest probability should occur. If that course of action does not occur, then the defender is surprised. While probability based surprise measurements might be appropriate for modeling or simulations, they do not appear useful for operational planning. This is because probability based surprise measurements normally rely on an assumption that the attacker and defender are rational actors. History has shown that rational actor assumptions do not necessarily mesh well with armed conflict. Therefore, the hypothesis utilizes a different approach to measure the effects of surprise, time. Time is the measure of effectiveness for deliberate surprise attacks.

Two of the authors researched, Leonhard and Simpkin, used time to measure surprise. Leonhard offers an easy to understand explanation of this relationship between time and surprise. In the Leonhard model, the attacker will surprise the defender if he can attack the defender before the defender achieves a state of readiness sufficient to stop the attack. During the first phase of the Leonhard model, the attacker wants to delay the defender's detection of the attacker for as long as possible. Once detected, if detected, the attacker wants to hasten contact as quickly as possible. This "hastening to contact" further ensures that the attacker catches the defender unprepared and by surprise. Simpkin adds a little more to this basic model.

In Simpkin's model, both the attacker and the defender experience four general phases to their operations: pre-executive (planning phase), pre-movement (preparation phase), movement (deployment phase), and executive (employment phase). To Simpkin, the attacker can achieve

the effects of surprise during the first two phases and maybe even the third. Simpkin further explains that the attacker loses strategic surprise once he enters the defender's territory, and he loses operational surprise once the defender deduces the attacker's objectives. ToSimpkin, as with Leonhard, operational tempo is a key to achieving surprise.[20]

The hypothesis uses a combination of both models. Furthermore, the hypothesis expresses the measurement in terms of the defender's ability to counter the attacker's surprise operation. By doing this the TTP can develop measurements appropriate for both the attacker and the defender. It is compatible for the attacker's perspective because the total amount of time it takes the defender to counter the surprise operation is the total amount of time available to the attacker for exploitation. It is appropriate for the defender's perspective because the total time it takes the defender to react represents a measurement of the defender's system efficiency, that is, slower reaction time represents higher defender ISR system, IM system, Decision Making system, and possibly countermeasure inefficiencies.

In this surprise model, time starts when the attacker gives the attack order. Time stops when the defender has effectively countered the attack. If the defender never effectively counters the surprise attack, he will remain surprised until he can develop an effective countermeasure. Described in other terms, the total time available to the attacker to exploit the defender's information gap is the total measure of effectiveness. Table 4 below provides a breakout of the time measurements in an attempt to clarify the concept.

[20] Richard E. Simpkin, *Race to the Swift, Thoughts on Twenty-First Century Warfare*(New York, New York: Brassey's Defence Publishers, 1985), 183.

Table 4. Surprise Effects Measurement	
1.	Time it takes defender's ISR system to plan, direct, collect, process, exploit, produce, and disseminate relevant information (warning indicators)
2.	Time it takes the relevant information to makes its way through the defender's information management system and arrive at the defender's decision making system
3.	Time it takes the defender to plan, decide upon and order an effective countermeasure
4.	Time it takes the order to make its way to the countermeasure force
5.	Time it takes the defender's countermeasure force to deploy
6.	Time it takes the defender's countermeasure to execute an effective countermeasure

Essentially, the times added in Table 4 equal the total time available for the attacker to exploit surprise. This could work well for planning because it gives the planner an estimate of the time that the defender will be surprised. If the attacker needs more time to mass or maneuver, he must increase the duration of his offensive IO effects. An airborne assault forcible entry operation provides an illustrative example of this concept. If the ground commander estimates that it will take his forces two hours to assemble on the drop zone and mass to a desired 80 percent combat effectiveness level, the offensive IO planner knows that he will need to provide the ground commander at least two hours of surprise effects. Two hours is the measure of effectiveness, anything short of two hours is mission failure for the offensive IO planner.

Summary

Chapter 4 advanced the surprise hypothesis by introducing a planning and executionTTPs for the attacker. The TTP described task and purpose formulation, an effects based operations methodology to achieve surprise, and a way to measure the effectiveness of surprise operations. The attacker must achieve the effects of surprise before he can exploit surprise. Offensive IOare the key. Offensive IO creates the conditions necessary for surprise that in turn allow the attacker the opportunity to exploit the surprise and gain the initiative on the battlefield. This chapter focused on the attacker's side of the equation. Chapter 5 discusses the other side of the surprise equation and the second component of surprise, defender information gaps.

CHAPTER 5

Defender Information Gaps, the Second Component of Surprise

Thus far, the monograph has shown how information gaps create opportunities for surprise. Now the discussion turns to the explanation of *why* information gaps are a problem for the defender. This understanding is critical to fully grasping the concept of surprise. Unfortunately, this explanation is wholly absent from current military doctrine. Chapter 5 provides one explanation that addresses the issue.

Defender ISR and IM systems are complex and adaptive. Additionally, these defender systems will not normally sit idle while the attacker has his way. They will change, they will attempt to restore information superiority equilibrium, and they will attempt to survive. However, why do the systems not adapt? What is causing the devastating effects on the defender systems? The answer to all of these questions, from an IS point of view, is straightforward. The roots of the defender's problems are assumptions, hypotheses, and biases. This is the focus for the chapter.

As the deliberate surprise attack unfolds, the defender has a problem. He needs relevant information, but the attacker has degraded or destroyed the defender's ISR and IM systems. The defender needs to know the attacker's intentions and capabilities. This is the only way to produce effective countermeasures to the attack. What does the defender do? The defender must make assumptions to fill the information gaps. These assumptions become the basic building blocks for hypotheses. To produce the necessary countermeasures, the defender must hypothesize about the attacker's intentions and capabilities. Now, the defender walks a road fraught with even further disaster. His assumptions, hypotheses, and planning is now subject to even further problems called biases.

Most in the military are generally familiar with and have heard the pitfalls associated with hypothesis creation and usage. Moreover, everyone in the military has heard at one time or another that thoughts and plans are subject to bias, and perhaps remember a few points from a basic psychology class taken many years ago. However, few in the military know exactly what this all means and the implications to these biases. Military manuals do not explain biases, and military classrooms do not teach these concepts. However, to understand the link among information gaps, assumptions, hypotheses, biases, and surprise, planners must understand the basic psychology underlying the concepts. The remainder of this chapter highlights psychological pitfalls associated with planning in an environment of information gaps.

To describe some of the problems associated with hypotheses and biases, the discussion relies on Richards J. Heuer's award winning book, *Psychology of Intelligence Analysis.* While Mr. Heuer focused his attention toward intelligence analysts, his findings, research, and experience appear relevant to surprise as well. These findings are consistent with the conclusions developed by at least five other authors researched for this project: Betts, Knorr, Morgan, Daniel, and Herbig. By summarizing Heuer's work, the analysis further highlights the relationship between information gaps and surprise. This is the defender's side of the surprise equation.

Problems with Hypotheses

Generating and Evaluating Hypotheses

Situational Logic. This approach assumes that each situation is unique. The defender, beginning with the known facts, will normally focus on establishing a cause-effect or means-end relationship. He determines the attacker's goals and then attempts to determine the ways and means the attacker will use to achieve these goals. The approach has two problems. First, the defender must be intimately familiar with the attacker's values, assumptions, misperceptions, and

misunderstandings--nearly an impossible task. Secondly, if the defender uses this approach solely, he gives up the opportunity to incorporate historical and theoretical information.[21]

Applying Theory. Based upon his understanding of how the attacker's individuals, institutions, and systems normally behave, the defender applies personal knowledge to the situation at hand. Aside from the fact that the defender might be dead wrong, this approach usually fails to tie predicted events to a timeline and may cause the defender to ignore relevant information. Planners and leaders normally apply this approach in an environment of time pressure and ambiguity, the conditions normally associated with a surprise attack.[22]

Reasoning by Comparison or Analogy. The defender compares the current situation to an analogous situation in history. The more the current situation is similar to the historical situation the better. When information gaps occur, the defender fills the gaps with his understanding of the historical event. In this case, the defender assumes that the same factors are at work, the outcomes of both situations will be similar, and or the course of action that worked in the past is likely to work again. The dangers are obvious. The two situations may very well not be similar. The course of action that worked in the past may very well not be appropriate to the current situation. The defender is likely to use this methodology when he lacks a theory sufficient to explain the current situation.[23]

Data Immersion. A final method is to attempt to inspect the incoming information with absolute objectivity. That is, review the data until a pattern emerges. This is a theoretical ideal but impossible in reality. Information becomes relevant information through human analysis. The analyst, whether staff member or decision maker, always filters the data through his personal lens tainted with assumptions, preconceptions, and expectations. The removal of the brain of the

[21] Richards J. Heuer Jr., *Psychology of Intelligence Analysis*. <http://www.odci.gov/csi/books/19104/index.html> (10 January, 2002).
[22] Ibid.
[23] Ibid.

analyst is the only way to prevent this from happening. Data Immersion is highly desirable, but impossible to achieve.[24]

Choosing Hypotheses

Satisficing. In this case, the defender starts with an answer that appears to best fit the situation. As he collects information, he separates the information into a group that supports the original answer and another group that contradicts the original hypothesis. At the end, the defender would quickly review all of the data that did not fit the original hypothesis to eliminate any glaring contradictions. Unfortunately, this approach has at least two problems. First, the defender naturally tends to find information he is looking for, that is the data that supports the original hypothesis. Second, he will automatically tend to be single focused. In other words, it becomes very difficult for the defender to change his original hypothesis event if it is wrong.[25]

Incrementalism. Once focused on a few different explanations, the defender will tend to make small adjustments around those explanations. It is very unlikely for the defender to make a large shift from his original supposition. People will not normally consider the need for drastic change from their original position.[26]

Consensus. Another dangerous way for the defender to choose a hypothesis is by choosing the hypothesis that will garner the most support. "Tell the boss what he wants to hear so we can all go home" is one example of this. The dangers are obvious, but it is very natural for military planners to consider this option in order to spur some kind of action. The defender could make a quicker decision, but that decision may order a very inappropriate countermeasure to the surprise attack.[27]

---

[24] Ibid.
[25] Ibid.
[26] Ibid.
[27] Ibid.

Analogy. This is a continuation of reasoning by comparison or analogy. The difference here is that the defender actually carried through with picking a course of action. He believes that what has worked in the past or in similar situations will work again and that is exactly what his countermeasure will be.[28]

Principles. This occurs when the defender conducts a course of action comparison based upon some preset fundamental(s). Does this sound familiar? Military organizations do this nearly every time the staffs and commanders evaluate their courses of action use the principles of war. Principles of war are probably not appropriate measures of effectiveness in many instances. If planners apply the principals of war without considering their validity as measures, they may fall victim to this error.

Failure to Reject Hypotheses. The scientific method seeks to reject hypotheses whereas military analysis does not necessarily follow this procedure. In fact, military analysis usually follows the complete opposite path. It naturally works to retain the hypotheses. This occurs because of various environmental factors, the lack of time is one example. The defender's systems will not naturally work to find disconfirming evidence. If the systems do find contradictory evidence, they will usually discount the information. "When information is processed in this manner, it is easy to 'confirm' almost any hypothesis that one already believes to be true."[29]

Problems with Biases

Perceptual

Once individuals or organizations see or understand something in a certain way, it is very difficult to change that view. If they have formed an erroneous view initially, it will take a considerable amount of discrepant information to force a correction to the initial false impression.

[28] Ibid.
[29] Ibid.

People will tend to assimilate as much of the contradictory information into the original view as possible. This bias is the normal reason that gradual, incremental change goes unnoticed. When the initial information available to the defender is limited and ambiguous, this bias poses a large problem. [30]

Probability Estimate

Availability. Succinctly put, the more readily one can remember or imagine an event taking place, the more likely that it can or may take place. This rule of thumb does often work well, but it is merely because of chance. This tool has little to do with the mathematical probability of an event occurring. This may be a very poor rule of thumb for the defender during surprise attacks...one that causes the defender to pay dearly.[31]

Anchoring. The defender will normally begin his estimate of the attacker's actions at some starting point or with some baseline analysis. It might be a previous estimate or it might be from some previous point in history. Normally, the defender's estimate will remain very close to the initial estimate varying very little as more information comes in. Analysts do not adjust their estimates enough. This initial baseline or estimate is like an anchor, hence the title.[32]

Overconfidence. In situations where the relevant information is low or the available information is ambiguous, the defender will have to rely on his subjective estimates. The defender provides his subjective best guess and this guess is usually based on an overestimation of the actual known information. This is a very precarious situation, but one that occurs very frequently.[33]

---

[30] Ibid.
[31] Ibid.
[32] Ibid.
[33] Richards J. Heuer Jr., "Cognitive Factors in Deception and Counterdeception," In *Strategic Military Deception*, Ed. Donald C. Daniel and Katherine L. Herbig (Elmsford, New York: Pergamon Press, Inc., 1981), 62.

Scenario Probability. In this situation defenders develop some likely scenario to explain the incoming information and attacker's actions. Mathematically, this approach has some problems. In general, people tend to believe that a correlation exists between details and probabilities, that is, the more detailed the scenario, the more probable the likelihood that the scenario will occur. They feel that the more details and pieces added to the puzzle, the more likely the chance it will occur. However, this violates mathematical probability laws. The likelihood of a scenario occurring is actually the probability of the least probable piece in the scenario (one of probability laws learned way back in high school).[34]

Evidence Evaluation

Oversensitivity to Consistency. "People have more confidence in conclusions drawn from a small body of consistent data than from a larger body of less consistent data."[35] The defender may disregard the fact that he is making judgments based upon a very small sample. Especially in an atmosphere with little information and little time to react. This is an observation particularly relevant for deception. This can prove to be very opportune if manipulated properly by the attacker.[36]

Absence of Evidence. While it would seem logical for the defender to be able to recognize his own information gaps and adjust his probability estimates accordingly, research indicates that this not the case. The defender is actually more likely to overlook, ignore, or not even recognize the problems with his availability of relevant information. Therefore, the attacker may in fact be exploiting an information gap that the defender is completely unaware. This case

---

[34] Richards J. Heuer Jr. *Psychology of Intelligence Analysis*. <http://www.odci.gov/csi/books/19104/index.html> (10 January, 2003).
[35] Richards J. Heuer Jr., "Cognitive Factors in Deception and Counterdeception," In *Strategic Military Deception*, Ed. by Donald C. Daniel and Katherine L. Herbig (Elmsford, New York: Pergamon Press Inc., 1981), 63.
[36] Richards J. Heuer Jr. *Psychology of Intelligence Analysis*. <http://www.odci.gov/csi/books/19104/index.html> (10 January, 2003).

may lead to complete surprise. The attacker would complete his surprise attack with no response from the defender.[37]

Vividness Criterion. This simply means that "vivid, concrete, and personal [information] has a greater impact on our thinking than pallid, abstract information." The danger is that the defender is more likely to incorporate vivid information, regardless of its value, as opposed to dull, monotonous potentially very valuable information, such as statistical data. In some cases, the defender will overlook, ignore, or minimize some very important relevant information, just because if fails the "vividness" test.[38]

Uncertain Accuracy. Most individuals in the defender's systems will use the evidence they have in memory to analyze the situation. The problem is that most people do not remember the source of the information or the original validity that they assigned to the information when they first received it. When dealing with information that has questionable reliability or accuracy, people tend to use two methodologies. In the first instance, they might use the "best guess" strategy. In this situation, people usually toss ambiguous information into one of two piles, the yes pile or the no pile. Information that ends up in the no pile is rarely re-looked. A second strategy is the "perfect and reduce" strategy. In this case, the defender will define perfect and then subjectively assign a lower than perfect value to the uncertain information. In both strategies, the result is statistical overconfidence in the analysis.[39]

Causality

Causal Explanation. In an attempt to impose order on the ambiguous situation, the defender is likely to establish causal patterns. However, this approach forces randomness, accidents, and error into explanations for observed events. If the defender cannot establish a pattern, then he will normally think that he has some how mentally erred. In the military, this is

[37] Ibid.
[38] Ibid.

the equivalent of attempting to assign causal relationships to the fog and friction of war. Sometimes, there is no logical explanation. This is another bias that could cloud the defender's judgment.[40]

Cause and Effect Similarity (also known as "Fallacy of Identity"). This occurs when the defender believes a similarity exists between the attributes of the cause and the attributes of the effect. Heuer provides the following examples when dealing with physical cause effect relationships: heavy things make heavy noises, dainty things move daintily, and large animals leave large tracks. This bias is normally correct in the case of physical properties, but may break down elsewhere.[41]

Overestimating Our Own Importance. This occurs when people give themselves much more credit than they realistically deserve. The bias could manifest itself when the defender believes his actions have a greater effect on the attacker than what they actually do. Possibly the U.S. believed that the power of its military would be enough to deter attacks on American soil. Terrorist actions on 11 September has changed the paradigm. It is very normal for people to overlook the simple fact that are other factors involved and other driving factors at play.[42] Militaries sometimes overlook the strength of environmental factors and variables.

Summary

It is important to understand the psychological aspects of surprise because this understanding opens the door to understanding the second component of surprise, defender information gaps. It is difficult to appreciate the link among surprise, information gaps, assumptions, hypotheses, and biases without the general understanding of the pitfalls associated with hypotheses and biases. When the attacker attacks the defender's information gaps, the defender is in a predicament. The defender needs the relevant information that his ISR and IM systems are not providing. The

---

[39] Ibid.
[40] Ibid.
[41] Ibid.

clock is ticking, and the defender must provide an effective countermeasure to the surprise attack. His only option is to assume and hypothesize about the attacker's intentions and capabilities, but his assumptions and hypotheses put him in even more jeopardy. Now, all of the defender's planning and countermeasures are subject to numerous biases. This worsens his situation. Meanwhile the attacker has attained the effect of surprise, he will then exploit theses effects and gain the initiative on the battlefield. The defender must accept his fate.

[42] Ibid.

CHAPTER 6

It Might Work, the Siren's Song

The goal in this monograph was to develop a surprise hypothesis suitable for argument and testing. The hypothesis had to meet several criteria. First, it had to develop a clear and concise definition of surprise. Second, the research needed to determine and describe the components of surprise. Third, the hypothesis had to include a visual model depicting the relationship among surprise and its components. The fourth goal was to develop a TTP suitable for an attacker to plan and execute deliberate surprise attacks. Finally, the monograph had to explain the relationship among the hypothesis pieces while remaining consistent with current doctrine. This monograph achieved the goal and met the hypothesis creation criteria by linking the principle of war surprise and information superiority.

Surprise and information superiority are directly related. Surprise is the attacker exploitation of defender information gaps. The two surprise components are exploitation and information gaps. Both components must be present in order to achieve the effects of surprise. Using the effects based operational construct, the military can plan, execute, and measure the effects of deliberate surprise operations. The hypothesis is sound and is prepared for the next step in the Scientific Method, testing.

Can operational and tactical planners use this hypothesis in their planning and execution right now? Yes, they could. Planners do not have to wait for doctrine to catch up. The hypothesis is adequate, feasible, acceptable, and compatible with Army and joint doctrine. Discussion has already shown that the hypothesis can work with the effects based operations methodology. Additionally, this hypothesis seems quite compatible with Army transformation programs and objective force initiatives. It may even bolster some of the underlying arguments to some of those concepts. Information operations doctrine has come a long way. The understanding and appreciation of IO throughout the force will continue to improve with time.

Recommendation 1: Finish the Scientific Method

This research process must continue to the hypothesis testing stage of the Scientific Method. Once tested, the hypothesis can become a sound theory and the basis for doctrinal change. The military has at least three different methods to accomplish this task. The first method is to submit the hypothesis to case study analysis. Submitting the hypothesis to historical fact allows necessary revision and refinement of the hypothesis. The second method is to circulate the monograph within the doctrine writing community in order to generate argument. This will subject the hypothesis to a more rigorous expert review. Finally, the U.S. military must distribute this idea to the field for input after the case study analysis and doctrine community revision. Great minds within the force may have already pondered this problem.

Recommendation 2: Principles of War Handbook

To understand the principles of war, the officer and soldiers must understand the theory and historical events supporting the principles of war. While this information does not need to be in doctrinal publications, the information does need to be some place readily accessible. A handbook that includes the definition, components, visual models, theory and history, and planning TTPs for each of the principles of war would go along way toward achieving this goal.

Recommendation 3: Recommended Reading

Planners must read Richards J. Heuer Jr.'s book *Psychology of Intelligence Analysis.* Mr. Heuer developed this book for intelligence analysts and intelligence managers. However, it is very applicable to planners in all of the services. This book explains nearly every mental fallacy that a planner could possibly encounter during the planning processes. To defend against fallacious preconceptions, assumptions, biases, and planning shortcuts, planners have to be able to recognize them. Mr. Heuer explains how to recognize the pitfalls. This book would probably fit best into the critical thinking and reasoning section of the curriculum of the Advanced Military Studies Program curriculum.

Recommendation 4: Simulations Improvement

Simulations must incorporate surprise. The probability method of measuring surprise might provide a way to incorporate surprise into our simulations. A formal review of information theory, communication theory, and gaming theories could determine the appropriate path. These theories may or may not provide the formulas suitable for modeling and simulating surprise in computer exercises. A formal review would answer these questions.

Recommendation 5: Staff Structure Review

Military staff structures must adjust to recognize the importance of information superiority. Information superiority is at least as important as maneuver and logistics in full spectrum operations. FM 3-0 has recognized the importance of information superiority. However, current staff structures might not be organized as efficiently as possible to support information dominance. For example, the three primary contributors to information superiority are ISR, under the G2; IM, predominately under the purview of the G6; and IO, which is spread throughout the staff. A possibly more efficient staff structure would add a Deputy Commander for Information Superiority (ADC-IS). Reporting to the ADC-IS would be the G2, G6, and the additional staff position of the G7. The G7 would be the staff primary for IO. This staff reorganization could prove to be more efficient than our current ad hoc method of Targeting Boards and IO planning cells. A formal review would determine the proper combination.

Appendix A: A Short History of Surprise Theory

Other Military Theorists

Sun Tzu

Can Sun Tzu's writings in his book *The Art of War* written 2,500 years ago be of any use to the twenty-first century American military? The answer is not really. Sun Tzu recognizes the importance of surprise and provides some conclusions, but he does not provide any type of theoretical underpinnings. Like the rest of his work, Sun Tzu explains rules of thumb. Military commanders can follow these rules of thumb and win battles or they can ignore Sun Tzu's warnings and lose. He does not explain his thought process. Sun Tzu tells you how to surprise, but not why or how it works.[43]

Frontinus

Frontinus was a Roman politician and diplomat who lived around A.D. 75. He was a prolific writer, and his works on surprise and stratagem were especially renowned. Unfortunately, Frontinus does not provide a theory of surprise either. However, *The Strategems* does contribute to surprise in two other major ways. First, his book was a "how to" guide for surprise and strategem. All means, methods, and concepts of surprise operations have a parallel found in Frontinus' writings. His stories advocate searching out and attacking weakness. To attack where unexpected, when unexpected, and with unexpected methods is the best course of action with Frontinus. These exact concepts continue to live in modern surprise doctrine definitions. Furthermore, Frontinus encourages attacking along a line of alternate objectives. By pursuing this strategy, the attacker forces the defender to split and dilute his forces in order to protect multiple objectives. With the enemy forces split, the attacker may now mass your forces at the

[43] Sun Tzu, *The Art of War*, Translated by Samuel B. Griffith (New York: Oxford University Press, 1971), 69.

point of his choosing and gain relative combat power at that point. Liddell Hart advocates this exact strategy in his modern-day writings. Frontinus repeats this concept of "desensitization" in *The Strategems*.[44] Frontinus describes numerous accounts where Roman generals deliberately conducted repetitive operations at the same time of day, at the same place, with the same methods in order to cause the enemy to drop his guard. Today, the name of this situation is the "Cry Wolf Syndrome." This simple, effective ploy is very relevant in modern military operations. The Egyptians used this tactic to desensitize the Israelis in 1973, the U.S. military used this ploy to desensitize Noriega's forces prior to Operation Just Cause, and the U.S. successfully used the concept again to desensitize Sadam's forces prior to Operation Desert Storm (the Marine's repetitive amphibious operation exercises in the Persian Gulf). Beyond surprise methods, Frontinus highlights the legality of surprise operations or with the Romans, the illegality.

Frontinus stresses that Roman surprise operations had no limit. Taking politicians hostage, throwing the severed adversary heads into crowds, poisoning water supplies, and poisoning food supplies were all part of the Roman repertoire. The Roman stories remind Western militaries of why surprise operations have moral and legal limits. Additionally, the stories highlight that many techniques unavailable to the U.S. conventional military are quite readily available to terrorists and those types of organizations. *The Stratagems* is a dream book for terrorists and a horror story for U.S. Homeland Defense.

Vegetius

Thoughts on surprise do not change throughout the Age of Antiquity. Romans continued to look for and attack weaknesses. They also continued to skirt the boundaries of morality. In A.D. 390, Vegetius summarizes Roman beliefs by stating that, "It is much better to overcome the enemy by famine, surprise or terror than by general actions, for in the latter instance fortune has

[44] Frontinus, *The Stratagems*, Trans. by Charles E. Bennet (Cambridge, MA: Harvard University Press, 1969), 99.

often a greater share than valor."[45] The end of Antiquity ends military thought in general through the Dark and Middle Ages.

Machiavelli

Machiavelli lived during the Italian period of diplomacy, "an age of constant warfare, of alliance and counter-alliance, or assassination and coup d'etat."[46] The Italian city-states depended on citizen armies, blackmail, and treachery for survival. In the spirit of true Roman tradition, politics and military endeavors had no legal or moral limits. One would expect that Machiavelli of all people would provide some answers to the research questions, but he does not. He describes the life of the resource constrained Italian city-states and their willingness to use the quickest and most cost effective means available to secure quick victory. Surprise was merely a tool. "Trickery, depending upon secrecy, deception, and surprise [were] axiomatic to the political theory of Machiavelli."[47] Machiavelli further clarifies his position in *The Discourses* by stating, "Although to use fraud in all one's actions is detestable, nevertheless in carrying on war it is praiseworthy and brings fame: he who conquers the enemy by fraud is praised as much as he who conquers them by force."[48]

Frederick

Frederick needs little introduction. He "carried the operations of ancient war to the highest degree of perfection they ever attained," and believed "ruses of war [to be] of great usefulness."[49] He liked to attack on a line of alternate objectives and attack vulnerable points along the enemy lines of communications (LOC). More importantly, Frederick is the first theorist to link surprise

---

[45] Renaus Flavius Vegetius, *The Military Institution of the Romans*, Trans. by Lieutenant John Clarke, Vol. 2, *Roots of Strategy* (Pennsylvania: Stackpole Books, 1985), 172.

[46] Niccolo Machiavelli, *The Art of War,* Trans. by Ellis Farneworth (Cambridge, MA: Da Capo Press Books, 1965), xi.

[47] Ibid, lviii.

[48] Niccolo Machiavelli, *Machiavelli: The Chief Works and Others,* Trans. by A. Gilbert. *The Discourses*, Vol 1 (Durham, NC: Duke University Press, 1965), 518.

[49] Frederick, *The Instruction of Frederick The Great for His Generals (1747)*, Trans. by Brig. Gen, Thomas R. Phillips, *Roots of Strategy*, Vol. 1, (Pennsylvania: Stackpole Books, 1985), 351.

and information. Surprise provided his small forces advantage and initiative. Information provided the surprise. He is also the first to bring out the idea of achieving surprise by exploiting enemy preconceptions, beliefs, and biases--a concept that becomes important later with the review of the civilian sector works. Finally, Frederick understood that in order to keep the enemy from surprising him, he must keep his information from the enemy. He believed in this so much that he was largely purported to be a bit of an operations security (OPSEC) fanatic. Frederick would even keep his plans from his generals and staff until the last minute. Luckily, this OPSEC method has fallen out of vogue. However, Frederick's OPSEC fanaticism seems to have carried over to his theories on surprise. He does not provide any.

Jomini

Unfortunately, Jomini was not a great supporter of expending resources chasing after surprise. "The surprise of an army is now next to an impossibility....Prearranged surprises are rare and difficult because in order to plan one it becomes necessary to have an accurate knowledge of the enemy's camp."[50] However, he does tie surprise to knowledge. Furthermore, Jomini did not downplay the value of surprise. In fact, he appreciated a good surprise operation when it happened, but would never advocate squandering valuable resources in pursuit of a surprise that might not ever materialize. That sums up Jomini.

Von Leeb

Von Leeb agrees with Clausewitz that speed and secrecy are the components of surprise, but he adds another, the concept of exploitation. Von Leeb explains that, "Rapidity is an essential condition for surprise. If one does not act promptly, usually the enemy is not surprised. He has time to take counter measures."[51] This is a very short phrase holding a great deal of meaning. First, he ties the concept of exploitation to surprise. That is, if the attacker does not exploit the

---

[50] Baron Antoine-Henri de Jomini, *The Art of War (*Philadelphia, PA: J. B. Stackpole Books, 1996), 209.

effects of surprise, he has done nothing except jump out of a closet and yell, boo. The defender will quickly realize that he has been caught off guard. The defender will correct the deficiency and thus slam the door on the initiative the attacker temporarily possessed. The second concept Von Leeb brings to light concerns time. Surprise has a temporal characteristic to it. Surprise does not last forever. Beyond these two points, Von Leeb adds nothing to the discussion of surprise.

Erfurth

So important were Erfurth and his book that society all but forgot him and his book when the world entered World War II. He explains what Clausewitz meant by speed and the relationship between speed and secrecy: "If a military decision is executed with the utmost speed, the chances are that the enemy will be surprised. Secrecy and speed are mutually dependent upon each other. If secrecy cannot be maintained, speed must be increased; if speed is not practical, the enemy must be kept wholly ignorant of the impending operations. Otherwise surprise can never be achieved."[52] Erfurth picks up the torch from Clausewitz and adds one more component to surprise, the ability to move.[53] The book also highlights the relationship between surprise and information.

"Surprise does not depend upon lack of care or complete ignorance on the part of the enemy. To achieve surprise, it is no means necessary that the enemy dreams or sleeps, but that one undertakes an operation which he does not expect."[54] Throughout his book, Erfurth illuminates the linkage between surprise and information. He describes how erroneous assumptions, biases, preconceptions, experience, and incorrect expectations all play a part in fertilizing an

---

[51] Ritter Von Leeb, *Defense*, Trans. by Dr. Stefan T. Possony and Daniel Vilfroy, *Roots of Strategy,* Vol. 3 (Pennsylvania: Stackpole Books, 1991), 117.
[52] Waldemar Erfurth, *Surprise*, Trans. by Dr. Stefan T. Possony and Daniel Vilfroy, *Roots of Strategy*, Vol. 3, (Pennsylvania: Stackpole Books, 1991), 393.
[53] Ibid., 553.

[54] Ibid, 359.

environment to grow opportunities for surprise. Erfurth writes how commanders will attempt to dominate their environments through information superiority in an attempt to reach a state of omniscience. Of course, no commander or organization will ever reach this state. Information gaps will always exist and planners will have to fill these gaps with hypotheses and assumptions. Frequently, these best guesses will be wrong and this incorrect information will provide an opportunity for exploitation.

B. H. Liddel Hart

The author of thirty military books, a former British Army captain and a military correspondent for the *London Times*, Liddell Hart and his writings remain firmly entrenched in all current military debates throughout the Western world. Hart does not explore the theory of surprise. He, rather, accepts its importance and constructs an entire strategic theory based in part on surprise. The main driving purpose of Hart's theory is "to diminish the possibility of resistance, and it seeks to fulfill this purpose by exploiting the elements of movement and surprise."[55] Mathematically, he describes his strategy with this formula: *Strategy = Movement + Surprise*. By way of narrative, he describes the relationship among strategy, movement, and surprise as follows:

> Although strategy may aim more at exploiting movement than at exploiting surprise, or conversely, the two elements react on each other. Movement generates surprise, and surprise gives impetus to movement. For a movement which is accelerated or changes its direction inevitably carries with it a degree of surprise, even though it be unconcealed; while surprise smoothes the path of movement by hindering the enemy's counter-measures and counter-movements.[56]

To Hart, surprise is both a principle of war and a vital element of war. Militaries must do more than "hope it happens." Military organizations have to take actions to ensure it happens and they must further recognize that surprise is part of any worthy strategy.

---

[55] B. H. Liddell Hart, *Strategy*, 2nd rev. ed. (New York, New York: Penguin Books USA INC., 1967), 323.
[56] Ibid.

Richard E. Simpkin

In his book, *Race to the Swift*, Simpkin reviews military theory under the context of the mid-1980s. During this era, the largest concerns to the military community were the nuclear threat from the Soviet Union and the increased militarization of Third World conflicts. In his chapter on surprise and strategems, Simpkin states his position on surprise, "Actions which depend on surprise, such as raids (in the Western sense), are essentially based onmanoeuvre theory."[57] This hints that he will also be basing his theory of surprise on speed. That is in fact the case. The interesting point in Simpkin's case is that he discounts the "secrecy" component normally found in military theories of surprise. He believes that it is all but impossible to keep operations hidden. Simpkin bases this belief on the mere fact that as a plan is passed down the chain of command, hundreds upon hundreds of people have access to the plan and it is simply impossible to prevent leaks in this type of environment.[58] Beyond this, Simpkin provides a few more points on surprise.

First, relying almost verbatim on J. F. C. Fuller's theory of surprise, Simpkin provides two definitions based on two possible types of surprise, moral surprise and material surprise: "**Moral surprise** means that the enemy does no know you are coming; in Fuller's view, only moral surprise can achieve an immediate decision....**Material surprise** means that the enemy knows you are coming but cannot do anything to stop you."[59]

Unfortunately, this view of surprise is rather narrow and discounts other types of surprise, like technical (new weapon systems) surprise. His more important contribution comes about when he describes one method to quantify material surprise using time. To summarize his theory, Simpkin basically says that an attacker achieves surprise because his decision and execution cycle is farther along the time continuum than a defender's decision and execution cycle. In other words, because an attacker has already planned and is usually in the midst of executing a surprise

[57] Richard E. Simpkin, *Race to the Swift, Thoughts on Twenty-First Century Warfare*(New York, New York: Brassey's Defence Publishers, 1985), 181.
[58] Ibid., 190.

attack by the time the defender discovers the attack, the attacker has gained the initiative and surprised the defender.[60] Thus, the time between when attacker begins planning for an operation and the time that the operation is disclosed to the defender (normally during execution) is the amount of surprise that the attacker has achieved on the defender.

Simpkin also sees a use for moral surprise with relation to the economy of force principle. Restated, a planner who is planning a surprise operation can use a smaller than normal correlation of force ratio when planning his operation. The planner can do this because the defender will be caught in a state of unreadiness. Simpkin mathematically portrays this state of unreadiness by explaining that the attacker will normally catch the defender at a 60 to 80 percent state of readiness during a surprise attack. Therefore, the planner can use 20 to 40 percent less forces to achieve the same combat power ratios that he would need for an operation that does not include surprise.[61]

COLONEL T. N. Dupuy

Unfortunately, Dupuy does not do anything for surprise but provide a definition. Additionally, research cannot determine if Dupuy made this definition or if he took it from the existing military manuals of the time. Either way, this definition is an early attempt at a definition and is very similar to current military definitions of surprise.

> *Surprise may decisively shift the balance of combat power in favor of the commander who achieves it*. It consists of striking the enemy when, where, or in a manner for which he is unprepared. It is not essential that the enemy be taken unaware but only that he becomes aware too late to react effectively. Surprise can be achieved by speed, secrecy, deception, by variation in means and methods, and by using seeming impossible terrain. Mass is essential to the optimum exploitation of the principle of surprise.[62]

---

[59] Ibid., 182.
[60] Ibid., 183.
[61] Ibid., 184.
[62] T. N. Dupuy, *Understanding Defeat: How to recover from loss in battle to gain victory in war* (Falls Church, VA: Nova Publications, 1990), 252.

Like existing military definitions of surprise shown in the chapter 1, this definition does everything but define surprise. Dupuy's definition tells why surprise is important and lists some of the methods militaries might use to achieve surprise. While the younger generations should applaud Colonel Dupuy for presenting a definition, his definition is confusing and everything but clear and concise.

Other Doctrinal Publications

Joint Doctrine

Joint doctrine does not discuss anything pertaining to surprise beyond the definition. Specifically, the following manuals do not mention anything about surprise other than the occasional platitude confirming the importance of surprise:

- Joint Publication (JP) 1-0, *Joint Warfare of the Armed Forces of the United States*
- JP 0-2, *Unified Action Armed Forces*
- JP 3-0, *Doctrine for Joint Operations*
- JP 5-0, *Doctrine for Planning Joint Operations*
- JP 5-00.1, *Joint Doctrine for Campaign Planning*
- JP 5-00.2, *Joint Task Force Planning Guide and Procedures*

Additionally, surprise did not even make the list for JP 1-02, *Department of Defense Dictionary of Military and Associated Terms.*

Army Doctrine

Field Manual (FM) 5-0 (101-5), *Army Planning and Orders Production* (Initial Draft), and Field Manual 6-0, *Command and Control* (DRAG Draft), have little to offer for this research. Research did uncover a relevant obsolete manual. Published in 1988, FM 90-2 *Battlefield Deception*, was the premier and probably only military manual ever produced that addressed the psychological effects of warfare. The manual made a valiant attempt to promote deception as a viable tool in the American warrior's toolbox. Unfortunately, deception dropped out of the

mainstream doctrine shortly after its publication. This work displayed the tight relationship among deception, OPSEC, and surprise. Put in other terms, it showed the importance of attacking enemy information, protecting friendly information, and exploiting weaknesses in enemy information. While providing the early day deception techniques, the book also describes the unbreakable bond between deception and surprise.

Marine Corps Doctrine

Marine Corps Doctrinal Publication (MCDP) 1, *Warfighting*, and MCDP 1-2, *Campaigning*, are the two primary Marine surprise manuals. MCDP 1-1, *The Study of Strategy*, and the Marine Corps Warfighting Publication 5-1, *Marine Corps Planning Process*, also address the subject. The Marines recognize surprise as a necessary precondition of superiority and genuine source of combat power.[63] They further recognize the components of surprise as speed, stealth, ambiguity, and deception.[64] One way to reword this is to say speed (Clausewitz), secrecy (Clausewitz), poor ISR, and IO without loosing any of the points the Marine manuals intended to make. Additionally, the Marines recognize the temporal characteristics of surprise: "Its advantages are only temporary and must be quickly exploited."[65] Marine manuals make one final point. The point is that: "Surprise is not what we *do*; it is the enemy's *reaction* to what we do. It depends at least as much on the enemy's susceptibility to surprise--his expectations and preparedness. Our ability to achieve surprise thus rests on our ability to appreciate and then exploit our enemy's expectations."[66]

---

[63] Ibid., Marine Corps Doctrinal Publication 1, *Warfighting* (Washington, DC: HQs Department of the Navy, 20 June 1997), 42.
[64] Ibid., 43.
[65] Ibid.
[66] Ibid.

Other Civilian Sector Works

Whaley

Whaley's book *Strategem, Deception and Surprise in War,* is a landmark statistical study. It is the only mathematical analysis ever attempted on surprise. He uses the scientific method to analyze 93 conflicts from across the globe between 1914 and 1968 to develop statistically supportable conclusions. The first conclusion relevant to this study is that surprise is composed of four factors: secrecy, preconception, deception, and response time. Below are other interesting conclusions:

- From 1914-1968, 73% of all cases that had deception resulted in surprise.[67]

- The most common mode in which surprise appears is place (or direction), being present in 72% of all instances of surprise studied. Place is closely followed by time (66%) and strength (57%), tailed by intention (33%), and ended by style, which was present in only 25% of all instances of surprise.[68]

- To cite only the extremes: Out of 59 battles fought without any initial surprise, only 2% substantially exceeded its general's expectations while 60% ended in abject failure.[69]

- [Strategem] has at least an 80% chance of yielding surprise.[70]

- The more intense the surprise, the more favorable the casualty ratios. The empirical data quite emphatically verifies this.[71]

Whaley's statistics support one of his other conclusions, that surprise and deception are bedfellows. It is extremely difficult to have one without the other and "only a small repertoire of strategems are needed to insure surprise after surprise."[72] The discussion closes with Whaley's

---

[67] Barton Whaley, *Strategem, Deception and Surprise in War* (Cambridge, MA: Center for International Studies, MIT, 1969), 156.
[68] Ibid., 214.
[69] Ibid., 215.
[70] Ibid., 234.
[71] Ibid., 194.
[72] Ibid., 228.

observation of the U.S. military's attitude toward surprise: "Moreover, it is the U.S. authorities who from the 19th Century to 1968 have consistently gone against the international trend by rating surprise toward the bottom of their scales."[73] It seems that the U.S. military force's disregard for this principle of war has at least been consistent throughout the ages.

Daniel and Herbig, *Strategic Military Deception*

While it may seem odd and confusing for the research to divert into the realm of deception, it is not. In his book *Strategem, Deception and Surprise in War,* Whaley proves beyond argument that deception and surprise are most assuredly related. Therefore, by studying *Strategic Military Deception*, planners can hope to find some tips on surprise. Another reason for reviewing this study is that *Strategic Military Deception* was a military sponsored multidisciplinary investigation of deception. It was the first organized attempt to study deception. It seems the recent surprise-filled Arab-Israeli wars may have sparked interest with the U.S. military giant. In this book, editors and team leaders Donald C. Daniel and Katherine L.Herbig explore deception with relation to several other contemporary theories (Table A1).

Table A1. Other Relevant Theories	
1	Cognitive Theory
2	Organizational Theory
3	Communications Theory
4	Game Theory
5	Systems Theory

The outcomes from these examinations are completely different from that found with military theorists. In this study, surprise originates from the manner in which individuals, groups, and organizations treat information, handle (or better put, mishandle) information, and the ways in

[73] Ibid., 126.

which they interact with each other. For example, biases, perceptions, prejudices, groupthink, organization goals, and interagency competition are all factors leading to surprise. The book also highlights the need for a feedback channel.[74] This is the only way an attacker can determine if his surprise operations are working and the only way he will be able to retain some control over a deliberate surprise operation. Without a feedback channel, the attacker will still probably achieve your surprise, but he will not know it until long after the operation. This situation occurred frequently in the early ages of war. Early warriors would unknowingly conduct and reap the benefits from surprise operations.

Betts, *Surprise Attack, Lessons for Defense Planning*

Sponsored by the Brookings Institution, Richard K. Betts wrote *Surprise Attack* in 1982 in an attempt to analyze the relationship between strategic surprise and defense policy. Betts defines surprise "in terms of the defender's unreadiness, caused by one or more mistaken estimates of whether, when, where, and how the enemy [will] strike."[75] He goes on to make another important point that, "Surprise in itself is unimportant. Indeed, anything unexpected is a surprise."[76] In military parlance, this means that surprise unexploited is worthless. Roughly interpreted, Betts sums up the causes of strategic surprise as:

- The defender does not know whether the enemy will attack.
- The defender does not know when the enemy will attack.
- The defender does not know where the enemy will attack.
- The defender does not know how the enemy will attack.[77]

The book has two recurring thematic causes of surprise throughout: (1) the attacker's use of the initiative to frustrate the victim's capacity to interpret warning indicators (a breakdown in the

[74] Donald C. Daniel and Katherine L. Herbig, *Strategic Military Deception* (Elmsford, New York: Pergamon Press Inc., 1981), 8.
[75] Richard K. Betts, *Surprise Attack, Lessons for Defense Planning* (Washington, DC: The Brookings Institution, 1982), 11.
[76] Ibid., 10.

ISR system), and (2) the organizational impediments to timely decision and response by the victim's command and control (a breakdown in information management and decision-making systems).[78] Again, the civilian interpretation of surprise components differs from the military theorist surprise components of secrecy and speed.

Knorr and Morgan, *Strategic Military Surprise, Incentives and Opportunities*

This book takes a wholly different approach to the topic of strategic military surprise, but generally concludes along the same lines as Betts. EditorsKnorr and Morgan define strategic military surprise in terms of its purpose. They state, "The purpose of a strategic attack is to inflict a striking defeat that sharply alters the military situation and possibly determines the outcome of the conflict."[79] As the title indicates, this book puts forth two components of surprise, incentive and opportunity. The attacker must have an incentive to conduct a surprise attack, and the defender must present an opportunity for such an attack. The book reaches the following conclusions (shown in Table A2). These are also the necessary conditions for a surprise attack:

Table A2. Necessary Conditions for Strategic Surprise Attack

ATTACKER		DEFENDER	
1	Must be motivated to conduct a surprise attack	1	Ambiguous information amidst a "noisy" environment
2	Must be willing to decide to conduct a surprise attack	2	Preconceptions and expectations different from reality
3	Must detect an exploitable defender weakness suitable to surprise attack	3	Organizational barriers to accurate perception
4	Must be willing to invest the time and resource necessary for the attack	4	Organizational barriers to effective response
5	Secrecy	5	Political constraints on what a government can afford to see and do
6	Deception		

Source: Klaus Knorr and Patrick Morgan, eds., "Strategic Surprise: An Introduction," In *Strategic Military Surprise* (New York, NY: National Strategy Information Center, Inc., 1983), 240.

[77] Ibid., 4.
[78] Ibid., 87.
[79] Klaus Knorr and Patrick Morgan, eds., "Strategic Surprise: An Introduction," In *Strategic Military Surprise* (New York, New York: National Strategy Information Center, Inc., 1983), 1.

While these are most assuredly valid at the strategic level of war, they are also readily transferable to the operational level of war.

Kam, *Surprise Attack*

Ephraim Kam wrote *Surprise Attack* in 1988. He was perplexed why surprise attacks continue to succeed. It seems logical that with the exponential growth of communications and technologies available to the modern day nation-state that surprise would not continue to be a viable military alternative. In his quest, Kam attacks the problem at four angles: the individual intelligence analyst, the small group of analysts, the intelligence community, the military organization, and the decision makers. To a military force, this could be interpreted as the interaction between the commander, his ISR system, and his information management system. By choosing the victim's perspective, Kam uncovers the internal problems with the four groups discussed above that allow the surprise attack to happen. Kam does not attempt to define surprise, but he does define what he calls the concept of surprise. He does this by explaining his components of surprise:

- A military act that violates the victim's expectations and assumptions.

- A failure of advance warning.

- The victim's failure to effectively counter the attack.[80]

In military lexicon, this could be termed as the exploitation of the enemy's information inferiority, a breakdown in the ISR system, and a break down in the information management system.

Kam concludes that with the three major reasons for successful surprise attacks. First, is the poor quality of information and data available to predict the enemy's intent andcapabilities. Second, is the persistence of conceptions even in the face of contradictoryevidence. Finally, Kam explains what he terms interdependence. He further explains this phenomenon as a

[80] Ephraim Kam, *Surprise Attack* (Cambridge, MA: Harvard University Press, 1988), 8.

cascading reaction where one wrong hypothesis creates a negative reaction throughout the entire system.[81] It is probably easiest to understand Kam's conclusions by reviewing his recommendations to fix the problems that he discovered (shown in Table A3 below).

Table A3. Remedies for the Surprise Attack			
ANALYTICAL PROCESS		ORGANIZATIONAL PROCEDURES	
1	Increase awareness of limitations	1	Improve information collection
		2	Reduce group influence; establish a devil's advocate
2	Improve hypotheses development	3	Establish pluralistic intelligence agencies
		4	Improve the warning system
3	Improve information processing	5	Improve relationship between intelligence community and decision makers

Source: Ephraim Kam, *Surprise Attack* (Cambridge, MA: Harvard University Press, 1988), 216.

[81] Ibid, 214.

Appendix B: Data Tables and Screening Discussions

Definition Screening

Table B1. Raw Definition Data	
Fuller & Simpkin[a]	Moral surprise means that the enemy does no know you are coming.
	Material surprise means that the enemy knows you are coming but cannot do anything to stop you.
Dupuy[b]	Surprise may decisively shift the balance of combat power in favor of the commander who achieves it. It consists of striking the enemy when, where, or in a manner for which he is unprepared. It is not essential that the enemy be taken unaware but only that he becomes aware too late to react effectively. Surprise can be achieved by speed, secrecy, deception, by variation in means and methods, and by using seeming impossible terrain. Mass is essential to the optimum exploitation of the principle of surprise.
Leonhard[c]	Surprise is a condition in which a military force is contacted while in a relative state of unreadiness.
	Surprise is a battlefield condition that results from the interaction of two components: perpetual unreadiness and time.
JP 3-0[d]	The purpose of surprise is to strike the enemy at a time or place or in a manner for which it is unprepared. Surprise can help the commander shift the balance of combat power and thus achieve success well out of proportion to the effort expended. Factors contributing to surprise include speed in decision-making, information sharing, and force movement; effective intelligence; deception; application of unexpected combat power; OPSEC; and variations in tactics and methods of operation.
FM 3-0[e]	Strike the enemy at a time or place or in a manner for which he is unprepared. Surprise is the reciprocal of security. Surprise results from taking actions for which an enemy or adversary is unprepared. It is a powerful but temporary combat multiplier. It is not essential to take the adversary or enemy completely unaware; it is only necessary that he become aware too late to react effectively. Factors contributing to surprise include speed, information superiority, and asymmetry.
MCDP 1[f]	*MCDP 1*. By surprise, we mean a state of disorientation resulting from an unexpected event that degrades the enemy's ability to resist. We achieve surprise by striking the enemy at a time or place or in a manner for which the enemy is unprepared. It is not essential that we take the enemy unaware, but only that awareness came too late to react effectively. The desire for surprise is more or less basic to all operations, for without it superiority at the decisive point is hardly conceivable.
Betts[g]	Anything unexpected is a surprise.
Kam[h]	A military act that violates the victim's expectations and assumptions.
Merriam Webster[i]	An attack without warning.
	To attack unexpectedly.
	To capture by an unexpected attack.

	Stresses causing an effect through being unexpected at a particular time or place.

Sources: [a] Richard E. Simpkin, *Race to the Swift, Thoughts on Twenty-First Century Warfare* (New York, NY: Brassey's Defence Publishers, 1985), 182.
[b]T.N. Dupuy, *Understanding War: History and Theory of Combat* (Falls Church, VA: Nova Publications, 1987), 252.
[c]Robert R. Leonhard, *Fighting by Minutes, Time and the Art of War* (Westport, Connecticut: Praeger Publishers, 1994), 140. *The Principles of War for the Information Age* (Novato, CA: Presidio Press, Inc. 1998), 183.
[d]US Department of Defense, Joint Publication 3-0, *Doctrine for Joint Operations* (Washington, DC: Joint Chiefs of Staff, 10 September 2001), A-2.
[e]US Department of Defense, Field Manual 3-0, *Operations* (Washington, DC: HQ Department of the Army, June 2001), 4-14.
[f]US Department of Defense, Marine Corps Doctrinal Publication 1, *Warfighting* (Washington, DC: HQ Department of the Navy, 20 June 1997), 42.
[g]Richard Betts, *Surprise Attack, Lessons for Defense Planning* (Washington, DC: The Brookings Institution, 1982), 10.
[h]Ephraim Kam, *Surprise Attack* (Cambridge, MA: Harvard University Press, 1988), 8.
[i]*Merriam-Webster Online.* < http://www.m-w.com/> (11 October 2002).

FM 3-0

FM 3-0 states in part that surprise is the reciprocal of security. By definition, this statement is not quite true and is misleading. At first glance, the statement seems reasonable, but upon closer inspection breaks down. The most closely related FM 101-5-1 definition states that security is "a condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences."[82] The reciprocal of this definition would read something like a condition resulting from the elimination of protective measures that ensure a state of inviolability from hostile acts or influences. While this is an unenviable position, and this condition might come as a surprise to the defender, it is not necessarily surprise per say. It is probably more correct to term this condition defeat or a condition that exists just prior to an organization's defeat. Suffice it to say, that this statement from FM 3-0 is at least arguable. For this hypothesis, the definition will not contain contentious pieces of information; screening

[82] US Department of Defense, Field Manual 101-5-1/Marine Corps Reference Publication 5-2A, *Operational Terms and Graphics* (Washington, DC: HQs Department of the Army, 30 September 1997), 1-138.

eliminates this statement from consideration. The Marine Corps definition also has a few points worthy of closer inspection prior to their elimination from the updated definition.

MCDP 1

Two pieces of information remain to the MCDP 1 definition after initial screening, "a state of disorientation and the degradation of the enemy's ability to resist." Analysis begins by reviewing "a state of disorientation". The *Merriam-Webster Online* dictionary defines disorientation as the loss of bearing, loss of sense of time, loss of sense of place, or the loss of a sense of identity[83] While a defender might become disoriented in the command and control (C2) sense after being surprised, this is not a necessary condition to achieve surprise. The author's point is understandable. However, it is probably safe to eliminate this piece from the definition. The next phrase under review is: degrades the enemy's ability to resist.

As it stands, this is both true and untrue. Psychologically, historical instances abound where a good surprise operation caused a defender to flee. On the other hand, history also provides instances where surprise did not cause the defender to run. The Battle of the Bulge comes to mind. Furthermore, a defender's ability to resist also springs from his available combat power and freedom of action. For example, if an attacker strikes a defender at an unexpected location without doing anything to degrade his combat power and or his freedom of action, the surprise probably has done nothing to degrade his ability to resist. A more accurate rewritten statement is: temporarily degrades the enemy's C2 ability to apply his combat power. Nevertheless, this concept is an effect of surprise and is not an integral piece to an "essence" definition.

After the definition screening process, research has the following information remaining shown in Table B2 below.

[83] *Merriam-Webster Online.* < http://www.m-w.com/> (11 October 2002).

Table B2. Screened Definition Data	
Betts	Anything unexpected is a surprise.
Kam	A military act that violates the victim's expectations and assumptions.
Merriam Webster	To attack unexpectedly.
	To capture by an unexpected attack.
	Stresses causing an effect through being unexpected

Component Screening

Table B3. Raw Component Data	
Frederick[a]	Exploit defender erroneous preconceptions/beliefs/biases
	Secrecy
Clausewitz[b]	Secrecy
	Speed
Von Leeb[c]	Secrecy
	Speed
	Exploitation
	Time
Erfurth[d]	Secrecy
	Speed
	Maneuver
	Information Superiority
	Erroneous assumptions/preconceptions/experience/expectations
Hart[e]	Movement
Simpkin[f]	Speed
	Time
Dupuy[g]	Striking when the defender is unprepared
	Striking where the defender is unprepared
	Striking in a manner the defender is unprepared for
	Mass
Leonhard[h]	Perpetual unreadiness
	Time
	Delay detection
	Hasten to contact
JP 3-0[i]	Speed in decision-making
	Information sharing
	Force movement
	Effective intelligence
	Deception
	Application of unexpected combat power
	OPSEC
	Variations in tactics and methods of operation

FM 3-0[j]	Striking when the defender is unprepared
	Striking where the defender is unprepared
	Actions for which the enemy is unprepared
	Time
	Speed
	Asymmetry
FM 90-2[k]	Deception
	OPSEC
MCDP 1[l]	Striking when the defender is unprepared
	Striking where the defender is unprepared
	Speed
	Stealth
	Ambiguity
	Deception
	Exploit enemy expectations
Whaley[m]	Secrecy
	Preconception
	Deception
	Response time
Daniel & Herbig[n]	Biases/perceptions/prejudices
	Groupthink
	Organization goals
	Interagency competition
Betts[o]	Defender does not know whether the attacker will attack
	Defender does not know when the attacker will attack
	Defender does not know where the attacker will attack
	Defender does not know how the attacker will attack
	Exploitation
	ISR system breakdown
	Information management system breakdown
Knorr & Morgan[p]	Motivated to conduct surprise attack
	Willing to decide to conduct a surprise attack
	Detect exploitable defender weakness
	Secrecy
	Deception
	Ambiguous information within a "noisy" environment
	Erroneous preconceptions/expectations
	Organizational barriers to accurate perception
	Organizational barriers to effective response
	Political constraints on what a government can afford to see and do
Kam[q]	A military act
	The act violates the victim's expectation and assumptions
	Defender failure of advanced warning
	Defender failure to effectively counter the attack

Sources: [a]Frederick, *The Instruction of Frederick The Great for His Generals (1747)*, Trans. by Brig. Gen, Thomas R. Phillips, Vol. 1, *Roots of Strategy* (Pennsylvania: Stackpole Books, 1985), 352, 348.

[b]Carl Von Clausewitz, *On War*, Edited and translated by Sir Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 198.
[c]Ritter Von Leeb, *Defense*, Trans. by Dr. Stefan T. Possony and Daniel Vilfroy, Vol. 3, *Roots of Strategy* (Pennsylvania: Stackpole Books, 1991), 118-119.
[d]Waldermar Erfurth, *Surprise*, Trans. by Dr. Stefan T. Possony and Daniel Vilfroy, Vol. 3, *Roots of Strategy* (Pennsylvania: Stackpole Books, 1991), 353, 360, 373.
[e]B.H. Liddell Hart, *Strategy*, 2nd revised ed. (New York, NY: Penguin Books USA INC., 1967), 323.
fRichard E. Simpkin, *Race to the Swift, Thoughts on Twenty-First Century Warfare* (New York, NY: Brassey's Defence Publishers, 1985), 182-183.
[g]T.N. Dupuy, *Understanding War: History and Theory of Combat* (Falls Church, VA: Nova Publications, 1987), 252.
[h]Robert R. Leonhard, *The Principles of War for the Information Age* (Novato, CA: Presidio Press, Inc. 1998), 183. *Fighting by Minutes, Time and the Art of War* (Westport, Connecticut: Praeger Publishers, 1994), 140.
[i]US Department of Defense, Joint Publication 3-0, *Doctrine for Joint Operations* (Washington, DC: Joint Chiefs of Staff, 10 September 2001), A-2.
[j]US Department of Defense, Field Manual 3-0, *Operations* (Washington, DC: HQs Department of the Army, June 2001), 4-14.
[k]US Department of Defense, Field Manual 90-2, *Battlefield Deception* (Obsolete) (Washington, DC: HQs Department of the Army, 3 October 1988), 20.
[l]US Department of Defense, Marine Corps Doctrinal Publication 1, *Warfighting* (Washington, DC: HQs Department of the Navy, 20 June 1997), 42.
[m]Barton Whaley, *Strategem, Deception and Surprise in War*, (Cambridge, MA: Center for International Studies, MIT, 1969), 152.
[n]Donald C. Daniel and Katherine L. Herbig, eds., *Strategic Military Deception*, (Elmsford, NY: Pergamon Press Inc., 1981). This is a collection of mini-studies. These surprise components are recurring themes throughout the work.
[o]Richard Betts, *Surprise Attack, Lessons for Defense Planning* (Washington, DC: The Brookings Institution, 1982), 4, 87, 92.
[p]Patrick Morgan, "The Opportunity for Strategic Surprise," In *Strategic Military Surprise*, Ed. by Klaus Knorr and Patrick Morgan (New York, NY: National Strategy Information Center, Inc., 1983), 195.
[q]Ephraim Kam, *Surprise Attack* (Cambridge, MA: Harvard University Press, 1988), 8.

ISR deficiencies and Information Management Deficiencies

Screening rewords "preconceptions, beliefs, biases, expectations, and perceptions" with "ISR/Information Management (IM) deficiency." This results from the following logic:

perceptions, beliefs, biases, and expectations occur because a defender makes assumptions, assumptions occur when a defender fills information gaps in order to continue planning, information gaps result from ISR and IM system deficiencies. The defender's information gaps occur because the defender's ISR system, usually for many very good reasons, is unable to fill the gap. The other possibility is that the defender has an information gap because relevant information has not reached the decision maker due to information management breakdowns. The next adjustment to the Raw Component Data concerns the third piece of IS, IO.

Secrecy and Information Operations

Secrecy and IO will not make the list of possible components. Nearly all authors hold secrecy as one of their components of surprise, keep your plans and actions secret from the enemy. Everyone in the military has heard this battle cry. Well, the description of secrecy and the current definition OPSEC are one in the same. FM 3-0 defines OPSEC as those actions that deny the enemy information critical to the success of friendly military operations. Furthermore, OPSEC is an information operation and IO are TTPs and methods designed to either increase or decrease IS depending upon which perspective is taken. TTPs and methods will not be a part of the component list. TTPs are ways to achieve surprise; they are not the necessary conditions that produce surprise. As a reminder, deception is also an IO. Therefore, screening eliminates deception from the component list.

Capability to Exploit Surprise

The screening process replaces all references to exploitation with the phrase: attacker exploitation. All of the information inputs reviewed stress the need to exploit the surprise. If you do not exploit surprise, you will let the initiative slip from your grasp. Therefore, speed, exploitation, time, maneuver, mass, hasten to contact, response time, and force movement are replaced with one statement: the attacker must have the ability to exploit and he must exploit the

opportunities provided by surprise before the enemy can recover from the surprise. This is "attacker exploitation".

Method Elimination

As previously discussed with IO, the surprise component list will not contain methods of achieving surprise. Attacking when, where, and with unexpected methods, asymmetry, and stealth are TTPs. They are methods that the attacker may use to achieve surprise. History has proven that some of these methods are very effective, but they are not constituent components of surprise. They are part-time players should the attacker decide to use them. Therefore, these too fail the screening tests.

Leonhard's Axiom of "Perpetual Unreadiness"

This axiom states that the ability to surprise arises from the concept that military units are perpetually unready. The attacker is betting that he can conduct his surprise operation faster than the defender can react to it. This axiom works well for most aspects of surprise, but appears to break down with technological surprise. An example is the Taliban ground forces at the outset of U.S. operations in Afghanistan. The Taliban could have been on a 100 percent alert status. Their early warning devices could have been deployed, employed, and operational. Their troops could have all been awake and manning their positions, but rest assured, the Taliban was indeed surprised when U.S. bombs began raining from the sky. This concept is no longer a contender.

Leonhard's "Delay Detection"

The component candidate list will not contain Leonhard's "delay detection." Delaying detection is secrecy in different clothing. Secrecy is OPSEC and OPSEC is an IO. The reader could also relate delaying detection to counterdeception, counterintelligence, or electronic protection that are all too IO. They are all IO methods, not essential components of surprise.

JP 3-0

JP 3-0 mentions speed in decision-making, effective information sharing, and effective intelligence. While desirable qualities necessary to efficient IM and ISR, they are not necessary components for surprise. The vast majority of conflicts operated under the conditions of poor information management and poor ISR compared to today's standards. Throughout history, thousands of examples exemplify surprise in this type of environment. Just by shear luck, it is possible for military organizations to achieve surprise with poor decision-making, ineffective information sharing, and ineffective intelligence. While these organizations probably did not exploit surprise, nothing prevented them from unknowingly achieving surprise.

MCDP 1

MCDP 1 posits ambiguity as part of the surprise equation. Ambiguity results from information gaps. Information gaps are the result of ISR and IM deficiencies. Thus, the phrase: ISR deficiency/Info Mgmt deficiency replaces the term ambiguity.

Daniel and Herbig

"Groupthink, organization goal conflicts, and interagency competition" become "Information Management deficiencies". Whether or not these are deficiencies, they can be at the very least information management challenges. Should these information management challenges go unresolved, they can clearly become deficiencies.

Betts

If a defender does not know whether, where, when, or how an attacker will attack, then the defender has serious, and potentially devastating information gaps. These gaps most probably result from either ISR or IM deficiencies. Hence, this concept is replaced with the phrase: ISR/IM deficiencies.

Knorr and Morgan

There are several required adjustments to the Knorr and Morgan raw component data. First, the attacker *does not* have to detect an exploitable weakness. The screening process already discussed this point. A military organization can surprise another military organization through shear luck. Secondly, "ambiguous information within a 'noisy' environment"are information gaps attributed to ISRand IM deficiencies. The monograph covered this link among information gaps, ISR deficiencies, and IM deficiencies earlier. Finally, "organizational barriers" and "political constraints" will not make the list. While ever present, these are environmental factors and not constituent surprise components.

Kam

As with the Knorr and Morgan data, the Kam raw component data requires several manipulations. First, the phrase "military act" has already been acknowledged. The new definition already includes the point. Secondly, the phrase "the act violates the victim's (defender's) expectations and assumptions" is renamed "ISR/IM deficiencies". The defender would not have had incorrect expectations and he would not have had to make assumptions if the ISR and IM systems were working properly in the first place. Next, advanced warning breakdowns are failures in the ISR and or IM systems. Finally, Kam suggests that the defender's inability to effectively counter an attack is a component of surprise. This is not a possible component. While this condition is a most welcome by-product or effect of surprise, it is not a component. For example, consider a recurring situation in Operation Northern Watch and Operation Southern Watch. Iraq most certainly knows that if it uses antiaircraft missile radars to "paint" coalition aircraft that the coalition aircraft will destroy the radar. While they cannot effectively counter coalition response, they are probably not surprised when the coalition conducts retaliation strikes. See Table B4 below for the final listing of screened component data.

Table B4. Screened Component Data	
Frederick	ISR deficiency/Info Mgmt deficiency
Clausewitz	Attacker exploitation
Von Leeb	Attacker exploitation
Erfurth	Attacker exploitation
	ISR deficiency/Info Mgmt deficiency
Hart	Attacker exploitation
Simpkin	Attacker exploitation
Dupuy	Attacker exploitation
Leonhard	Attacker exploitation
JP 3-0	Attacker exploitation
FM 3-0	Attacker exploitation
MCDP 1	Attacker exploitation
	ISR deficiency/Info Mgmt deficiency
Whaley	ISR deficiency/Info Mgmt deficiency
	Attacker exploitation
Daniel & Herbig	ISR deficiency/Info Mgmt deficiency
Betts	Attacker exploitation
	ISR deficiency/Info Mgmt deficiency
Knorr & Morgan	Attacker exploitation
	ISR deficiency/Info Mgmt deficiency
Kam	ISR deficiency/Info Mgmt deficiency

Task Screening

Targeting Objective

Table B5. Screened Targeting Objectives	
TARGETING OBJECTIVE	**DEFINITION & DESCRIPTION**
Deceive	Deceive is to cause a person to believe what is not true. Military deception seeks to mislead adversary decision makers by manipulating their understanding of reality. Successful deception causes them to believe what is not true.
Degrade	Degrade, in information operations, is using lethal or temporary means to reduce the effectiveness or efficiency of adversary command and control systems and information collection efforts or means. Offensive IO can also degrade the morale or a unit, reduce the target's worth or value, or reduce the quality of adversary decisions and actions.
Deny	Deny, in information operations, entails withholding information about Army force capabilities and intentions that adversaries need for effective and timely decision making. Effective denial leaves opponents vulnerable to offensive

	capabilities. Operations security (OPSEC) is the primary nonlethal means of denial. It applies throughout the spectrum of conflict.
Destroy	Destroy is to damage a combat system so badly that it cannot perform any function or be restored to a usable condition without being entirely rebuilt (FM 3-90). Destruction is most often the use of lethal and nonlethal means to physically render adversary information or INFOSYS ineffective unless reconstituted. It is most effective when timed to occur just before the adversary needs to execute a C2 function or when focused on a resource-intensive target that is hard to reconstitute.
Disrupt	Disrupt is a tactical mission task in which a commander integrates direct and indirect fires, terrain, and obstacles to upset an enemy's formation or tempo, interrupt his timetable, or cause his forces to commit prematurely or attack in a piecemeal fashion (FM 3-90). For IO, disruption involves breaking or interrupting the flow of information between selected C2 nodes. It may be desired when attack resources are limited, to comply with rules of engagement, or to create certain effects. Electronic attack is a common means of disrupting adversary C2 systems.
Exploit	Exploitation, in information operations, is covertly gaining access to adversary C2 systems to collect information or to plant false or misleading information.
Influence	Influence causes adversaries or others to behave in a manner favorable to Army forces. It results from applying perception management to affect the target's emotions, motives, and reasoning. Perception management also seeks to influence the target's perceptions, plans, actions, and will to oppose Army forces. Targets may include noncombatants and others in the AO whom commanders want to support friendly force missions or not resist friendly force activities. Perception management accomplishes the influences mission by conveying or denying selected information to targets.

Source: US Department of Defense, Field Manual 3-13, *Information Operations: Doctrine, Tactics, Techniques, and Procedures* (DRAG Draft) (Washington, DC: HQs Department of the Army, 9 November 2001), 1-13.

Formation

Table B6. Screened Formation Data	
JP 3-13.1[a]	Defender ISR system
	Adversary decisionmakers
	ISR system, IM system, decisionmaker, defensivie IO system, countermeasure force, links between the systems
FM 3-13[b]	Command and Control Systems
	Decisionmakers
	IM system
	ISR system

Sources: [a]US Department of Defense, Joint Publication 3-13.1, *Joint Doctrine for Command and Control Warfare (C2W)* (Washington, DC: Joint Chiefs of Staff, 7 February 1996), II-1, II-4, II-5, II-7.

[b]US Department of Defense, Field Manual 3-13, *Information Operations: Doctrine, Tactics, Techniques, and Procedures* (DRAG Draft) (Washington, DC: HQs Department of the Army, 9 November 2001), v, 2-2.

Function

Table B7. Raw Function Data	
Erfurth[a]	Ability to C2
	Ability to achieve relative superiority
	Ability to match attacker's tempo
	Ability to match attacker's decision making tempo
	Ability to determine relevant information
	Ability to Plan
	Ability to counter the attack
Hart[b]	Ability to counter the attack
Simpkin[c]	Ability to match attacker's decision making tempo
Dupuy[d]	Ability to react effectively
Leonhard[e]	Ability to counter the attack
	Ability to match attacker's tempo
	Ability to match attacker's decision making tempo
	Effectiveness of ISR system
JP 3-13.1[f]	Ability to C2
	Ability to match attacker's decision making tempo
	Effectiveness of ISR system
	Effectiveness of IM system
	Effectiveness of decision making system
	Ability to match attacker's tempo
	Ability to counter the attack
	Ability to achieve relative superiority
FM 3-0[g]	Ability to counter the attack
	Ability to determine relevant information
	Ability to C2
	Effectiveness of decision making system
	Ability to match attacker's tempo
	Effectiveness of ISR system
	Effective of IM System
FM 3-13[h]	Ability to C2
	Effectiveness of ISR system
	Effectiveness of decision making system
	Effectiveness of IM system
	Effectiveness of planning
MCDP 1[i]	Ability to counter the attack
Daniel & Herbig[j]	Effectiveness of ISR system
	Ability to determine relevant information
	Effectiveness of IM system
	Effectiveness of decision making system
Betts[k]	Effectiveness of decision making system

	Ability to counter the attack
	Effectiveness of decision making system
	Effectiveness of information management system
Knorr & Morgan[l]	Effectiveness of ISR system
	Effectiveness of IM system
	Effectiveness of decision making system
	Ability to achieve relative superiority
	Ability to determine relevant information
	Ability to counter the attack
Kam[m]	Ability to counter the attack
	Effectiveness of ISR system
	Ability to determine relevant information
	Effectiveness of decision making system

Sources:

[a]Waldermar Erfurth, *Surprise*, Trans. by Dr. Stefan T. Possony and Daniel Vilfroy, Vol. 3, *Roots of Strategy* (Pennsylvania: Stackpole Books, 1991), 393, 395-396, 427, 434, 509, 524.

[b]B.H. Liddell Hart, *Strategy*, 2nd revised ed. (New York, NY: Penguin Books USA INC., 1967), 323.

[c]Richard E. Simpkin, *Race to the Swift, Thoughts on Twenty-First Century Warfare* (New York, NY: Brassey's Defence Publishers, 1985), 182.

[d]T.N. Dupuy, *Understanding Defeat: How to recover from loss in battle to gain victory in war* (Falls Church, VA: Nova Publications, 1990), 252.

[e]Robert R. Leonhard, *The Principles of War for the Information Age* (Novato, CA: Presidio Press, Inc. 1998), 184. *Fighting by Minutes, Time and the Art of War* (Westport, CT: Praeger Publishers, 1994), 139-140.

[f]US Department of Defense, Joint Publication 3-13.1, Joint Doctrine for Command and Control Warfare (C2W) (Washington, DC: Joint Chiefs of Staff, 7 February 1996), v, I-1, I-6, I-7.

[g]US Department of Defense, Field Manual 3-0, *Operations* (Washington, DC: HQs Department of the Army, June 2001), 4-14, 7-9, 7-10, 7-12, 7-13, 11-6.

[h]US Department of Defense, Field Manual 3-13, *Information Operations: Doctrine, Tactics, Techniques, and Procedures* (DRAG Draft) (Washington, DC: HQs Department of the Army, 9 November 2001), v, vi, 1-3, 1-13, 1-14.

[i]US Department of Defense, Marine Corps Doctrinal Publication 1, *Warfighting* (Washington, DC: HQs Department of the Navy, 20 June 1997), 42.

[j]Donald C. Daniel and Katherine L. Herbig, eds., *Strategic Military Deception*, (Elmsford, NY: Pergamon Press Inc., 1981), 71, 74, 78, 82, 89, 112, 136, 140, 358.

[k]Richard Betts, *Surprise Attack, Lessons for Defense Planning* (Washington, DC: The Brookings Institution, 1982), 16, 88, 90, 92, 102.

[l]Klaus Knorr and Patrick Morgan, eds., *Strategic Military Surprise* (New York, NY: National Strategy Information Center, Inc., 1983), 90, 195, 200, 204-205, 207-208, 210, 213, 226-227, 229-230, 232, 234, 237-238, 250, 251.

[m]Ephraim Kam, *Surprise Attack* (Cambridge, MA: Harvard University Press, 1988), 8, 12, 18-19, 31, 38, 72, 74, 78, 211.

Purpose Screening

Table B8. Raw Purpose Data	
Erfurth[a]	Economy of force
	Mass
	Maneuver
	Offensive
Hart[b]	Maneuver
Simpkin[c]	Maneuver
	Offensive
	Economy of Force
Dupuy[d]	Mass
	Mass
Leonhard[e]	Maneuver
	Maneuver
JP 1[f]	Mass
JP 3-13.1[g]	Offensive
	Mass
	Maneuver
FM 3-0[h]	Maneuver
	Mass
FM 3-13[i]	Offensive
MCDP 1[j]	Maneuver
	Mass
MCDP 1-1[k]	Mass
Whaleyl	Mass
Daniel & Herbig[m]	Offensive
Betts[n]	Mass
	Offensive
Knorr & Morgan[o]	Mass
	Maneuver
Kam[p]	Mass
	Maneuver
	Offensive

Source:
[a]Waldermar Erfurth, *Surprise*, Trans. by Dr. Stefan T. Possony and Daniel Vilfroy, Vol. 3, *Roots of Strategy* (Pennsylvania: Stackpole Books, 1991), 359, 367, 386, 396, 427, 502, 509, 524, 553.
[b]B. H. Liddell Hart, *Strategy*, 2nd rev. ed. (New York, NY: Penguin Books USA INC., 1967), 67.
[c]Richard E. Simpkin, *Race to the Swift, Thoughts on Twenty-First Century Warfare* (New York, NY: Brassey's Defence Publishers, 1985), 181-182, 184.

[d]T. N. Dupuy, *Understanding War: History and Theory of Combat* (Falls Church, VA: Nova Publications, 1987), 6. *Understanding Defeat: How to recover from loss in battle to gain victory in war* (Falls Church, VA: Nova Publications, 1990), 252.
[e]Robert R. Leonhard, *Fighting by Minutes, Time and the Art of War* (Westport, CT: Praeger Publishers, 1994), 139. *The Principles of War for the Information Age* (Novato, CA: Presidio Press, Inc. 1998), 192.
[f]US Department of Defense, Joint Publication 1, *Joint Warfare of the Armed Forces of the United States* (Washington, DC: Joint Chiefs of Staff, 14 November 2000), B-2.
[g]US Department of Defense, Joint Publication 3-13.1, *Joint Doctrine for Command and Control Warfare (C2W)* (Washington, DC: Joint Chiefs of Staff, 7 February 1996), vi, I-6.
[h]US Department of Defense, Field Manual 3-0, *Operations* (Washington, DC: HQs Department of the Army, June 2001), 4-14, 7-9.
[i]US Department of Defense, Field Manual 3-13, *Information Operations: Doctrine, Tactics, Techniques, and Procedures* (DRAG Draft) (Washington, DC: HQs Department of the Army, 9 November 2001), vi, 1-12.
[j]US Department of Defense, Marine Corps Doctrinal Publication 1, *Warfighting* (Washington, DC: HQs Department of the Navy, 20 June 1997), 38-39, 42-43.
[k]US Department of Defense, Marine Corps Doctrinal Publication 1-1, *The Study of Strategy* (Washington, DC: HQs Department of the Navy, 12 November 1997), 55.
[l]Barton Whaley, *Strategem, Deception and Surprise in War,* (Cambridge, MA: Center for International Studies, MIT, 1969), 196, 220.
[m]Theodore R. Sarbin, "Prolegomenon to a Theory of Counterdeception," In *Strategic Military Deception,* Ed. by Donald C. Daniel and Katherine L. Herbig (Elmsford, NY: Pergamon Press Inc., 1981), 151.
[n]Richard Betts, *Surprise Attack, Lessons for Defense Planning* (Washington, DC: The Brookings Institution, 1982), 14, 34, 89.
[o]Patrick Morgan, "The Opportunity for Strategic Surprise," In *Strategic Military Surprise,* Ed. by Klaus Knorr and Patrick Morgan (New York, NY: National Strategy Information Center, Inc., 1983), 200-201.
[p]Ephraim Kam, *Surprise Attack* (Cambridge, MA: Harvard University Press, 1988), 8, 12, 31.

Table B9. Screened Purpose Data	
1.	In order to allow the decisive operation to achieve economy of force
2.	In order to allow the decisive operation to maneuver
3.	In order to allow the decisive operation to mass
4.	In order to allow the decisive operation to achieve or maintain the offensive

Appendix C: IS, ISR, IM, IO Relationship Diagram

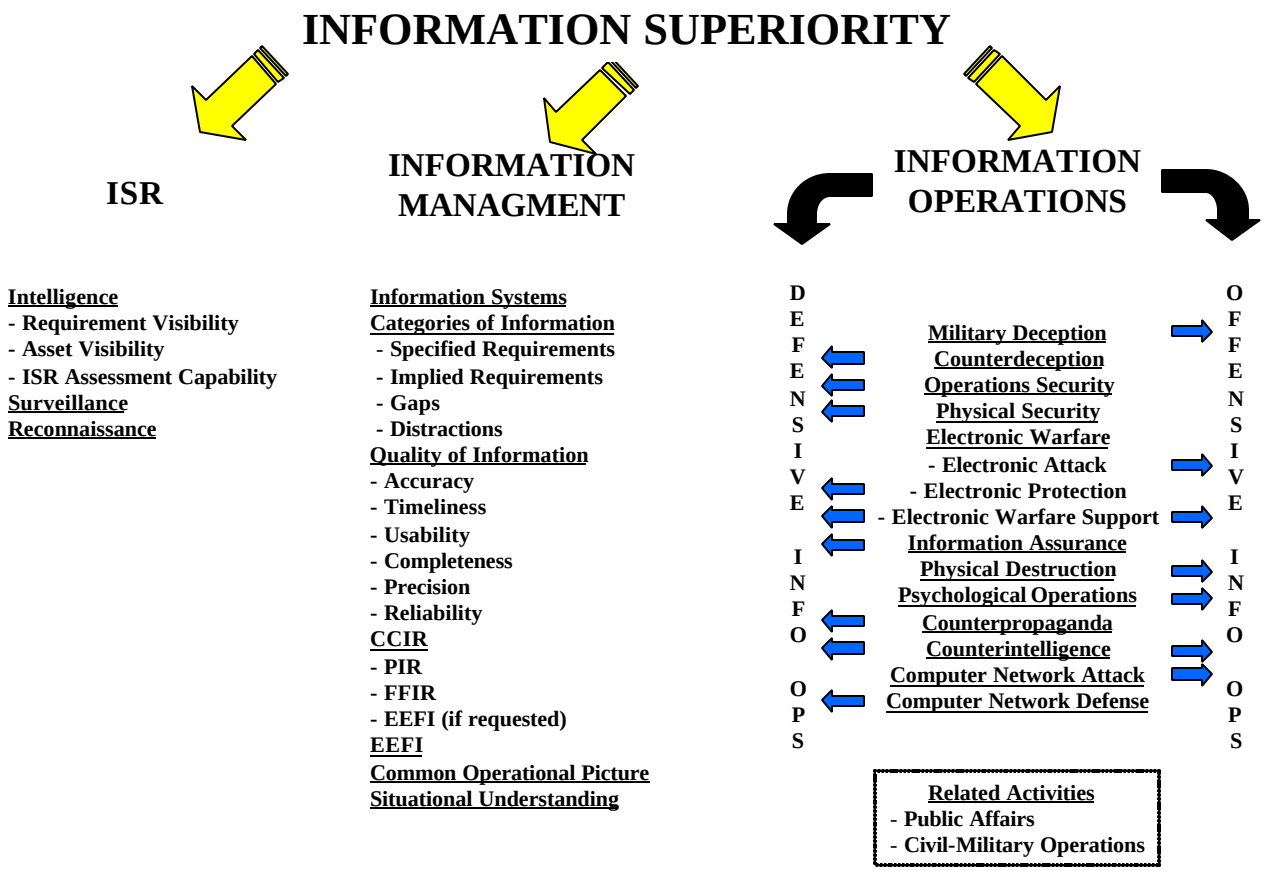

Figure C1. Information Superiority Summary

Appendix D: D3A and the Targeting Process Diagram

	Operations Process Activity	Targeting Process Activity	Targeting Task
ASSESSMENT	PLANNING	DECIDE	**Mission Analysis** • Develop IO-related HVTs • Provide IO input to targeting guidance and targeting objectives **COA Development** • Designate potential IO-related HPTs • Contribute to TVA • Deconflict and coordinate potential HPTs **COA Analysis** • Develop HPTL • Establish TSS • Develop AGM • Determine criteria of success BDA requirements **Orders Production** • Finalize HPTL • Finalize TSS • Finalize AGM • Submit IO IRs/RFIs to G2
	PREPARATION EXECUTION	DETECT	• Execute collection plan • Updated PIRs/ IO IRs as they are answered • Update HPTL and AGM
		DELIVER	• Execute attacks in accordance with the AGM
		ASSESS	• Evaluate effects of attacks • Monitor targets attacked with nonlethal IO

Source: US Department of Defense, Field Manual 3-13,*Information Operations: Doctrine, Tactics, Techniques, and Procedures* (DRAG Draft) (Washington, DC: HQs Department of the Army, 9 November 2001), E-2.

Glossary

NOTE: This is a summary of Information Superiority terms found in Chapter 11 Information Superiority, Field Manual 3-0, *Operations*. The author purposely chose a categorical listing method instead of the normal alphabetical listing procedures in order to ease the readers understanding of the terms and relationships among the terms.

Intelligence, Surveillance, Reconnaissance

Intelligence. (1) The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas; (2) information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding.

Requirements Visibility. Intelligence personnel use procedures and information systems to monitor and display the status of information requirements.

Asset Visibility. Intelligence personnel use procedures and information systems to monitor and display collection asset status, location, and activities.

ISR Assessment Capability. Intelligence personnel use procedures and information systems to assess the effectiveness of the ISR effort and the operational impact of ISR results (such as its success or gaps in collection), and to task collection assets.

Surveillance. The systematic observation of aerospace, surface or subsurface areas, places, persons, or things, by visual, aural, electronic, photographic or other means.

Reconnaissance. A mission undertaken to obtain by visual observation or other detection methods, information about the activities and resources of an enemy or potential enemy, or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area.

Information Management. The provision of relevant information to the right person at the right time in a usable form to facilitate situational understanding anddecision making. It uses procedures and information systems to collect, process, store, display, and disseminate information.

Information Systems. The equipment and facilities that collect, process, store, display and disseminate information. These include computers--hardware and software--and communications, as well as policies and procedures for their use.

Relevant Information. All information of importance to commanders and staffs in the exercise of command and control.

Categories of Information

Specified Requirements. Requirements the commander specifically identifies. This information may take the form of facts, estimates, or assumptions.

Implied Requirements. Important pieces of information that commanders have not specifically requested.

Gaps. Elements of information commanders need to achieve situational understanding but do not have...To fill gaps, commanders and staffs make assumptions.

Distractions. Information commanders do not need to know but continue to be told. Excessive distractions result in information overload.

Quality of Information

Accuracy. The information conveys the actual situation; in short, it is fact.

Timeliness. The information has not been overtaken by events.

Usability. The information is easily understood or displayed in a format that immediately conveys the meaning.

Completeness. The information contains all required components.

Precision. The information has the required level of detail, no more and no less.

Reliability. The information is trustworthy, uncorrupted, and undistorted.

Commander's Critical Information Requirements. Elements of information required by commanders that directly affect decision making and dictate the successful execution of military operations.

Priority Intelligence Requirements. Those intelligence requirements for which a commander has an anticipated and stated priority in his task of planning anddecision making.

Friendly Force Information Requirements. Information that the commander and staff need about the forces available for the operation.

Essential Elements of Friendly Information. The critical aspects of a friendly operation that, if known by the enemy, would subsequently compromise, lead to failure, or limit success of the operation, and therefore must be protected from enemy detection.

Common Operational Picture. An operational picture is a single display of relevant information within a commander's area of interest. A common operational picture is an operational picture tailored to the user's requirements, based on common data and information shared by more than one command.

Situational Understanding. The product of applying analysis and judgment to the common operational picture to determine the relationships among the factors of METT-TC.

Information Operations Definitions. Actions taken to affect adversary, and influence others', decision making processes, information and information systems while protecting one's own information and information systems.

Offensive Information Operations. The integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect enemy decision makers or to influence others to achieve or promote specific objectives.

Defensive Information Operations. The integration and coordination of policies and procedures, operations, personnel, and technology to protect and defend friendly information and information systems. Defensive information operations ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their won purposes.

Information Operations Elements

Military Deception. Measures designed to mislead adversaries and enemies by manipulation, distortion, or falsification. Its aim is to influence the enemy's situational understanding and lead him to act in a manner that favors friendly forces.

Counterdeception. Efforts to negate, neutralize, or diminish the effects of, or gain advantage from, a hostile deception operation. Counterdeception supports offensive IO by reducing harmful effects of enemy deception. Defensively, counterdeception identifies enemy attempts to mislead friendly forces.

Operations Security (OPSEC). Denies the enemy information critical to the success of friendly military operations. It contributes to the security of Army forces and their ability to surprise enemies and adversaries. OPSEC identifies routine activities that may telegraph friendly intentions, operations, capabilities, or military activities. It acts to suppress, conceal, control, or eliminate these indicators. OPSEC includes countersurveillance, signal security, and information security.

Physical Security. Prevents unauthorized access to equipment, installations, and documents. It safeguards and protects information and information systems.

Electronic Warfare (EW). Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. EW can cause an enemy to misinterpret the information received by his electronic systems. EW includes:

Electronic Attack. Actions taken to degrade, neutralize, or destroy enemy electronic combat capabilities. Actions may include lethal attack, such as antiradiation missiles and directed energy weapons, and nonlethal electronic attack, such as jamming.

Electronic Protection. Actions taken to protect friendly use of the electronic spectrum by minimizing the effects of friendly or enemy EW. Actions include radio silence and antijamming measures.

Electronic Warfare Support. Involves detecting, identifying, locating, and exploiting enemy signal emitters. It contributes to achieving situational understanding, target development and acquisition, damage assessment, and force protection.

Information Assurance. Protects and defends information systems. Threats to information systems include physical destruction, denial of service, capture, environmental damage, and malfunctions. Information assurance provides an enhanced degree of confidence that information and information systems possess the following characteristics: availability, integrity, authentication, confidentiality, and nonrepudiation. Computer network defense is part of this element.

Physical Destruction. Applies combat power against IO-related targets. Targets include information systems, EW systems, and command posts. Physical destruction that supports IO is synchronized with other aspects of the operation.

Psychological Operations (PSYOP). Planned operations that influence the behavior and actions of foreign audiences by conveying selected information and indicators to them. The aim of PSYOP is to create behaviors that support US national interests and the mission of the force. PSYOP are closely integrated with OPSEC, military deception, physical destruction, and EW to create a perception of reality that supports friendly operations.

Counterpropaganda. Includes activities directed at an enemy or adversary conducting PSYOP against friendly forces. Counterpropaganda can contribute to situational understanding and expose enemy attempts to influence friendly populations and military forces. Preventive actions include propaganda awareness programs that inform US and friendly forces and friendly populations about hostile propaganda.

Counterintelligence. Consists of activities that identify and counteract threats to security posed by espionage, subversion, or terrorism. It detects, neutralize, or prevents espionage or other intelligence activities. Counterintelligence supports the commander's requirements to preserve essential security and protect the force.

Computer Network Attack. Consists of operations that disrupt, deny, degrade, or destroy information resident in computers and computer networks. It may also target computers and networks themselves.

Computer Network Defense. Consists of all measures to defend computers and other components that are interconnected in electronic telecommunications networks against computer network attacks by an adversary. Such measures include access controls, detection of malicious computer code and programs, and tools to detect intrusions.

Related Activities. Related activities are distinct from IO because they do not manipulate or distort information; their effectiveness stems from their credibility with the local populace and news media.

Public Affairs. Operations influence populations by transmitting information through the news media. The fulfill the Army's obligation to keep the American people and the Army informed. Public Affairs help to establish conditions that lead to confidence in the Army and its readiness to conduct operations in peace, conflict, and war. Disseminating this information is desirable and consistent with security. Information disseminated through public affirs counters the effects of propaganda and misinformation.

Civil-Military Operations (CMO). Applies civil affairs to military operations. It encompasses activities that commanders take to establish, maintain, influence, or exploit relations between military forces and civil authorities--both governmental and nongovernmental--and the civilian populace. Commanders direct these activities in friendly, neutral, or hostile AOs to facilitate military operations and consolidate operational objectives....They promote the development of favorable emotions, attitudes, or behavior in neutral, friendly, or hostile groups.

Bibliography

NOTE: The author purposely chose to organize the bibliography to parallel the information input data group categories supporting the hypothesis instead of the normally accepted methodology in order to expedite and ease further research.

Military Theorists

Dupuy, T. N. *Understanding War: History and Theory of Combat.* Falls Church, VA: Nova Publications, 1987.

_____. *Understanding Defeat: How to Recover from Loss in Battle to Gain Victory in War*. Falls Church, VA: Nova Publications, 1990.

Erfurth, Waldemar. *Surprise*. Translated by Dr. Stefan T. Possony and Daniel Vilfroy. Vol. 3, *Roots of Strategy*. Pennsylvania: Stackpole Books, 1991.

Frederick. *The Instruction of Frederick The Great for His Generals (1747).* Translated by Brigadier General, Thomas R. Phillips. Vol. 1, *Roots of Strategy*. Pennsylvania: Stackpole Books, 1985.

Frontinus. *The Stratagems*. Translated by Charles E. Bennet. Cambridge, MA: Harvard University Press, 1969.

Hart, B. H. Liddell. *Strategy*, 2nd revised ed. New York, NY: Penguin Books USA, INC., 1967.

Jomini, Baron Antoine-Henri de. *The Art of War.* Philadelphia, PA: J. B. Lippincott, 1862.

Leonhard, Robert R. *Fighting by Minutes: Time and the Art of War*. Westport, CT: Praeger Publishers, 1994.

_____. *The Principles of War for the Information Age.* Novato, CA: Presidio Press, Inc., 1998.

Machiavelli, Niccolo. *The Art of War.* Translated by Ellis Farneworth. Cambridge, MA: Da Capo Press Books, 1965.

_____. *Machiavelli: The Chief Works and Others.* Translated by A. Gilbert. Vol. 1, *The Discourses*. Durham, NC: Duke University Press, 1965.

Simpkin, Richard E. *Race to the Swift: Thoughts on Twenty-First Century Warfare.* New York, NY: Brassey's Defence Publishers, 1985.

Sun Tzu. *The Art of War.* Translated by Samuel B. Griffith. New York: Oxford University Press, 1971.

Vegetius, Flavius Renatus. *The Military Institution of the Romans.* Translated by Lieutenant John Clarke. Vol. 2, *Roots of Strategy*. PA: Stackpole Books, 1985.

Von Clausewitz, Carl. *On War.* Edited and translated by Sir Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1976.

Von Leeb, Ritter. *Defense*. Translated by Dr. Stefan T. Possony and Daniel Vilfroy. Vol. 3, *Roots of Strategy*. PA: Stackpole Books, 1991.

Current doctrine

US Department of Defense. Field Manual 3-0, *Operations.* Washington, DC: HQs Department of the Army, June 2001.

_____. Field Manual 3-13, *Information Operations: Doctrine, Tactics, Techniques, and Procedures* (DRAG Draft). Washington, DC: HQs Department of the Army, 9 November 2001.

_____. Field Manual 5-0 (101-5), *Army Planning and Orders Production* (Final Draft). Washington, DC: HQs Department of the Army, 15 July 2002.

_____. Field Manual 6-0, *Command and Control* (DRAG Draft). Washington, DC: HQs Department of the Army, March 2001.

_____. Field Manual 90-2, *Battlefield Deception* (Obsolete). Washington, DC: HQs Department of the Army, 3 October 1988.

_____. Field Manual 101-5-1/Marine Corps Reference Publication 5-2A, *Operational Terms and Graphics*. Washington, DC: HQs Department of the Army, 30 September 1997.

_____. Joint Military Operations Historical Collection. Washington, DC: Joint Chiefs of Staff, 15 July 1997.

_____. Joint Publication 0-2, *Unified Action Armed Forces.* Washington, DC: Joint Chiefs of Staff, 10 July 2001.

_____. Joint Publication 1, *Joint Warfare of the Armed Forces of the United States.* Washington, DC: Joint Chiefs of Staff, 14 November 2000.

_____. Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms.* Washington, DC: Joint Chiefs of Staff, 12 April 2000 (As amended through 14 August 2002).

_____. Joint Publication 2-01, *Joint Intelligence Support to Military Operations.* Washington, DC: Joint Chiefs of Staff, 20 November 1996.

_____. Joint Publication 3-0, *Doctrine for Joint Operations.* Washington, DC: Joint Chiefs of Staff, 10 September 2001.

_____. Joint Publication 3-13.1, *Joint Doctrine for Command and Control Warfare (C2W)*. Washington, DC: Joint Chiefs of Staff, 7 February 1996.

_____. Joint Publication 5-0, *Doctrine for Planning Joint Operations.* Washington, DC: Joint Chiefs of Staff, 13 April 1995.

_____. Joint Publication 5-00.1, *Joint Doctrine for Campaign Planning*. Washington, DC: Joint Chiefs of Staff, 25 January 2002.

_____. Joint Publication 5-00.2, *Joint Task Force Planning Guide and Procedures.* Washington, DC: Joint Chiefs of Staff, 13 January 1999.

_____. Marine Corps Doctrinal Publication 1, *Warfighting*. Washington, DC: HQs Department of the Navy, 20 June 1997.

_____. Marine Corps Doctrinal Publication 1-1, *The Study of Strategy*. Washington, DC: HQs Department of the Navy, 12 November 1997.

_____. Marine Corps Doctrinal Publication 1-2, *Campaigning*. Washington, DC: HQs Department of the Navy, 1 August 1997.

_____. Marine Corps Doctrinal Publication 5-1, *Marine Corps Planning Process.* Washington, DC: HQs Department of the Navy, 12 November 1997.

Civilian Sector

Barnett, Sylvan, and Hugo Bedau, eds. *Critical Thinking, Reading, and Writing: A Brief Guide to Argument*. New York, NY: Bedford/St. Martin's, 1999.

Betts, Richard. *Surprise Attack: Lessons for Defense Planning.* Washington, DC: The Brookings Institution, 1982.

CNN Transcript. <http://www.cnn.com/TRANSCRIPTS/0109/11/bn.47.html> (2001).

Daniel, Donald C. and Katherine L. Herbig, eds. *Strategic Military Deception*. Elmsford, NY: Pergamon Press Inc., 1981.

_____. "Propositions on Military Deception." In *Strategic Military Deception.* Ed. by Donald Daniel and Katherine Herbig. New York: Pergamon Press Inc., 1982.

Dolphin, Lambert. "*Steps in the Scientific Method*." < http://www.ldolphin.org/SciMeth2.html> (2 May 1992).

Doyle, Michael. "Endemic Surprise? Strategic Surprises in First World-Third World Relations." In *Strategic Military Surprise.* Ed. by Klaus Knorr and Patrick Morgan. New York, NY: National Strategy Information Center, Inc., 1983.

Handel, Michael. "Crisis and Surprise in Three Arab-Israeli Wars."In *Strategic Military Surprise.* Ed. by Klaus Knorr and Patrick Morgan. New York, NY: National Strategy Information Center, Inc., 1983.

Heuer Jr., Richards J. "Cognitive Factors in Deception and Counterdeception." In *Strategic Military Deception.* Ed. by Donald C. Daniel and Katherine L. Herbig. Elmsford, NY: Pergamon Press Inc., 1981.

_____. *Psychology of Intelligence Analysis.* <http://www.odci.gov/csi/books/19104/index.html> (1999).

Kam, Ephraim. *Surprise Attack.* Cambridge, MA: Harvard University Press, 1988.

Knorr, Klaus. "Lessons for Statecraft." In *Strategic Military Surprise.* Ed. by Klaus Knorr and Patrick Morgan. New York, NY: National Strategy Information Center, Inc., 1983.

_____. "Strategic Surprise in Four European Wars." In *Strategic Military Surprise.* Ed. by Klaus Knorr and Patrick Morgan. New York, NY: National Strategy Information Center, Inc., 1983.

_____. "Strategic Surprise: The Incentive Structure." In *Strategic Military Surprise.* Ed. by Klaus Knorr and Patrick Morgan. New York, NY: National Strategy Information Center, Inc., 1983.

Knorr, Klaus and Patrick Morgan, eds. "Strategic Surprise: An Introduction." In *Strategic Military Surprise.* New York, NY: National Strategy Information Center, Inc., 1983.

Merriam-Webster Online. < http://www.m-w.com/> (11 October 2002).

Morgan, Patrick. "Examples of Strategic Surprise in the Far East." In *Strategic Military Surprise.* Ed. by Klaus Knorr and Patrick Morgan. New York, NY: National Strategy Information Center, Inc., 1983.

Moose, Paul H. "A systems View of Deception." In *Strategic Military Deception.* Ed. by Donald C. Daniel and Katherine L. Herbig. Elmsford, NY: Pergamon Press Inc., 1981.

Reese, William. "Deception in a Game Theoretic Framework." In *Strategic Military Deception.* Ed. by Donald C. Daniel and Katherine L. Herbig. Elmsford, NY: Pergamon Press Inc., 1981.

_____. "Deception within a Communications Theory Framework." In *Strategic Military Deception.* Ed. by Donald C. Daniel and Katherine L. Herbig. Elmsford, NY: Pergamon Press Inc., 1981.

Sarbin, Theodore R. "Prolegomenon to a Theory of Counterdeception." In *Strategic Military Deception.* Ed. by Donald C. Daniel and Katherine L. Herbig. Elmsford, NY: Pergamon Press Inc., 1981.

Shannon, C. E. "A Mathematical Theory of Communication." *The Bell System Technical Journal*, Vol. 27, July-October, 1948.

Sherwin, Ronald G. "The Organizational Approach To Strategic Deception: Implications For Theory And Policy." In *Strategic Military Deception.* Ed. by Donald C. Daniel and Katherine L. Herbig. Elmsford, NY: Pergamon Press, Inc., 1981.

Sherwin, Ronald G. and Barton Whaley. "Understanding Strategic Deception: An Analysis of 93 Cases." In *Strategic Military Deception.* Ed. by Daniel Donald C. and Katherine L. Herbig. Elmsford, NY: Pergamon Press, Inc., 1981.

Whaley, Barton. *Strategem, Deception and Surprise in War*. Cambridge, MA: Center for International Studies, MIT, 1969.