Strategy Research Project

Preventing Intelligence Failures in an Unpredictable 21st Century

by

Colonel Darin L. Brockington
United States Army

United States Army War College
Class of 2012

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
20-03-2012	Strategy Research Project	

4. TITLE AND SUBTITLE

Preventing Intelligence Failures in an Unpredictable 21st Century

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Colonel Darin L. Brockington

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Lieutenant Colonel John A.
Mowchan
Center for Strategic Leadership

8. PERFORMING ORGANIZATION REPORT NUMBER

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

U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution A: Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Intelligence is a fundamental element of national security; however, history is littered with intelligence failures. Intelligence is about gathering information to inform our decisions and make better choices. Ultimately, intelligence will always be imperfect and, as history demonstrates, surprise can never be completely prevented. Despite intelligence reform legislation enacted on December 17, 2004 to prevent another 9/11, the United States (US) intelligence community (IC) is guaranteed to experience intelligence failure(s) within the foreseeable future. The contemporary security environment presents a particularly difficult challenge for strategic intelligence warning. In the post-9/11 world, intelligence must move faster and leverage all sources of intelligence.

This paper proposes the current intelligence cycle model has major flaws. In short, the current intelligence cycle is not fast enough to keep up with, much less get ahead of, today's priority intelligence targets, which are greater in number and are often more obscure in character. The purpose of this paper is threefold: discuss the anatomy of intelligence; diagnose the general causes and consequences of intelligence failures; and prescribe an antidote for pathologies that contribute to failures.

15. SUBJECT TERMS

Surprise, Forecasting, Warning, Intelligence Community

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFED	UNCLASSIFED	UNCLASSIFED	UNLIMITED	32	

USAWC STRATEGY RESEARCH PROJECT

PREVENTING INTELLIGENCE FAILURES IN AN UNPREDICTABLE 21ST CENTURY

by

Colonel Darin L. Brockington
United States Army

Lieutenant Colonel John A. Mowchan
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Colonel Darin L. Brockington

TITLE: Preventing Intelligence Failures in an Unpredictable 21st Century

FORMAT: Strategy Research Project

DATE: 20 March 2012 WORD COUNT: 5,880 PAGES: 32

KEY TERMS: Surprise, Forecasting, Warning, Intelligence Community

CLASSIFICATION: Unclassified

Intelligence is a fundamental element of national security; however, history is littered with intelligence failures. Intelligence is about gathering information to inform our decisions and make better choices. Ultimately, intelligence will always be imperfect and, as history demonstrates, surprise can never be completely prevented. Despite intelligence reform legislation enacted on December 17, 2004 to prevent another 9/11, the United States (US) intelligence community (IC) is guaranteed to experience intelligence failure(s) within the foreseeable future. The contemporary security environment presents a particularly difficult challenge for strategic intelligence warning. In the post-9/11 world, intelligence must move faster and leverage all sources of intelligence.

This paper proposes the current intelligence cycle model has major flaws. In short, the current intelligence cycle is not fast enough to keep up with, much less get ahead of, today's priority intelligence targets, which are greater in number and are often more obscure in character. The purpose of this paper is threefold: discuss the anatomy of intelligence; diagnose the general causes and consequences of intelligence failures; and prescribe an antidote for pathologies that contribute to failures.

PREVENTING INTELLIGENCE FAILURES IN AN UNPREDICTABLE 21ST CENTURY

> It is not the strongest of the species that survive, nor the most intelligent, but the one most responsive to change.
>
> —Charles Darwin

All five types of intelligence—warning, current, analytic, research, and science & technology—are a fundamental element of national security. However, history is strewn with examples of intelligence failures and strategic surprise. The high incident of surprise throughout history is itself not surprising. If the Intelligence community (IC) fails to adapt to a fundamental change in technology, doctrine, or organization that renders existing methods of conducting warfare obsolete, it will likely result in another catastrophic strategic surprise. In fact, preventing strategic surprise has been a regularly recurring theme in United States (US) national security policy from at least the mid-20th Century to the present. For example, the modern IC has its origins in the aftermath of the intelligence failure at Pearl Harbor. The National Security Act of 1947 created the Central Intelligence Agency (CIA), America's first peacetime intelligence agency, and it also established a structure for the US national security that has persisted for 65 years. Consequently, indications and warning (I&W) intelligence was created to give advance notice to policymakers of potential futures and low probability/high impact scenarios. However, a recurring theme in this paper is that I&W intelligence will always be imperfect and, as history demonstrates, surprise can never be completely prevented.

Similar to the security situation in 1947, in the aftermath of the intelligence failure(s) that did not predict the terrorist attacks on 9/11, and the subsequent investigation by the 9/11 Commission, a movement grew to re-organize the IC in order

to prevent another 9/11-style terrorist attack. Consequently, the Congress legislated, and President George W. Bush signed the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) to provide more effective threat warning.[1]The IRPTA established the Office of the Director of National Intelligence (ODNI) to coordinate better the now 17 agencies, approximately 200,000 personnel, and about $75 billion in annual expenditures that comprise the sprawling U.S. intelligence community. Interestingly, the Director of National Intelligence (DNI) has turned over four times in its seven-year existence. The Honorable James R. Clapper is the current DNI.

Despite intelligence reform legislation enacted on December 17, 2004, to prevent another 9/11, the IC is guaranteed to continue experiencing intelligence failures within the foreseeable future. Most intelligence failures in the past were the result of systemic weaknesses in the way the IC collects, analyzes, and disseminates intelligence. Consequently, this paper proposes the current intelligence cycle model is flawed. Specifically, 10 years after 9/11, the IC is not adaptable enough to keep up with, much less get ahead of, today's priority intelligence targets (e.g. non-state actors, transnational criminal organizations, and terrorist groups), which are greater in number and more diffuse in character than ever before. The purpose of this paper is threefold: discuss the anatomy of intelligence; diagnose the general causes and consequences of intelligence failures; and prescribe an antidote for a pathology that contributes to intelligence failures. This paper will focus on improving finished intelligence used by the President and members of the policymaking, law enforcement, and military communities to make informed decisions or think strategically about long-term threats and opportunities.

Figure 1:

The U.S. Intelligence Community (IC) is a coalition of 17 agencies and organizations within the executive branch that work both independently and collaboratively to gather the intelligence necessary to conduct foreign relations and national security activities. Its primary mission is to collect and convey the essential information the President and members of the policymaking, law enforcement, and military communities required to execute their appointed duties.[2] Today, the IC is a large and complex organization. Its primary mission is clear-cut: to collect and convey essential information needed by the President and other consumers for the performance of their duties and responsibilities.[3]This includes collecting and assessing information concerning international terrorist and narcotic activities; other hostile activities by foreign powers, organizations, persons, and their agents; and foreign intelligence activities directed

against the US. To ensure it is performing these functions properly, the IC is subject to both Executive and Legislative oversight. Currently, “total” intelligence reform, as described by DNI Clapper in late 2010, is focused on “integration, the merging of collection and analysis—particularly at the national level—analytic transformation, analytic integrity, acquisition reform, counterintelligence, and information sharing.”[4]

The IC is responding to IRTPA mandated changes. Time will tell us if current intelligence reforms, brought about by the IRTPA, are evolutionary or revolutionary. Unfortunately, this paper posits intelligence reform and oversight are not a panacea. The demand for current intelligence on top-priority targets overwhelms analysts and collectors, detracting from long-term planning and efforts to think critically about future threats. History has repeatedly demonstrated that intelligence tradecraft practices, which do not detect, and adapt to emerging threats embedded in the international system, will likely result in more failures. As Richard Betts warned a few months after the terrorist attacks on 9/11, “the awful truth is that even the best intelligence systems will have big failures.”[5]When the world changes, the single most important requirement for intelligence is to change with it. Ultimately, intelligence professionals are held liable for the consequences of strategic surprise and the related problem of intelligence failure.

The Anatomy of Intelligence

Before one can begin to understand why intelligence fails, it is important to first define what intelligence is and what it is expected to accomplish. Debatably, the intelligence trade is the oldest profession in recorded history. Therefore, it is reasonable to expect to find a sophisticated description of just what that business is; what it does;

and how it works. However, defining intelligence is itself a complex question. There are almost as many definitions of intelligence as there are experts who have attempted to define it. As historian Walter Laqueur noted, so far no one has succeeded in crafting a theory of intelligence.[6]

The National Security Act of 1947 defines the kind of intelligence that we are seeking in this manner:

> The term 'foreign intelligence' means information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons.[7]

Study commissions appointed to survey the Intelligence Community have long used similar language. David T. Moore's influential paper titled, "Critical Thinking and Intelligence Analysis," provides this definition; "Intelligence is a "specialized form of knowledge…[that] informs leaders, uniquely aiding their judgment and decision-making.[8] [9] [10]"

And finally, the Central Intelligence Agency has weighed in with the following sentence:

> Reduced to its simplest terms, intelligence is knowledge and foreknowledge of the world around us—the prelude to decision and action by US policymakers.[11]

All of these definitions stress the "informational" aspects of intelligence more than its "organizational" facets. On the other hand, Sherman Kent expressed in a 1946 article on the contemporary direction of intelligence reform:

> The main difficulty seems to lie in the word 'intelligence' itself, which has come to mean both what people in the trade do and what they come up with. To get this matter straight is crucial: intelligence is both a process and an end-product.[12]

Sherman Kent identified and developed three concepts related to strategic intelligence: "knowledge" or what is produced and disseminated; "activity" or how such knowledge is

produced and disseminated; and “organization” or how people are grouped to produce and disseminate such knowledge.[13]While definitions vary, as used in this paper, “intelligence” refers to the process by which specific types of information important to national security are requested, collected, analyzed, and provided to policymakers to help illuminate their decision options. Knowledge, which is derived from analysis, is the only component of the strategic, operational, and tactical “intelligence triumvirate” that this paper addresses. Intelligence as an activity and organization lie beyond the scope of this paper.

There are four critical tasks to be successful at producing intelligence and preventing intelligence failures:

1. The intelligence collected must be timely and relevant.
2. The intelligence collected must be accurate.
3. The intelligence collected must identify risks and opportunities.
4. The intelligence collected must remain secret and be actionable.

The aim is to enable decision makers to make the best possible choices in the light of the facts and judgments sent to them. Since 1947, the practice of intelligence was to monitor threats from other nation states; that changed after 9/11 when the focus of much of the IC shifted to non-state actors. This paradigm shift is not surprising given the desire to prevent another 9/11; consequently, the number of dots that need to be connected expanded from a few nuclear capable countries to literally billions of individuals located in 196 countries around the world.

In sum, intelligence is about gathering information to inform our decisions and make better choices. During the ten years since 9/11, policymakers and military commanders have come to recognize the heightened priority and the central importance

of good intelligence in providing for the well-being, security, and defense of the US. Intelligence strives to ensure its findings are factual and — to the best knowledge of its creators —"true." The goal of intelligence is truth, but the quest for that truth "involves a struggle with a human enemy who is fighting back."[14]The attempted Christmas Day airplane bombing over Detroit on December 25, 2009, occurred more than eight years after 9/11; five years after the Iraq weapons of mass destruction (WMD) intelligence fiasco; and after countless commission reports, new congressional legislation, presidential executive orders, and other directives that diagnosed and sought to prevent such intelligence "failures" through widespread organizational, legal, policy, and tradecraft reforms. These ominous facts beg the question: is the IC better at preventing surprise following the post-9/11 reforms? To answer this question, one first requires an understanding of why intelligence fails.

The Causes and Consequences of Intelligence Failures

History is replete with intelligence failures. So prevalent have been these intelligence failures in the face of impending surprise attack that some analysts have even concluded that such failures are simply to be expected; as Betts put it, "intelligence failures are not only inevitable, they are natural."[15]Scholars of intelligence generally agree that intelligence analysts should not be expected to predict the future. Joseph Nye puts it this way: "the job of intelligence is not to predict the future, but to help policymakers think about the future."[16]In other words, intelligence is useful for providing estimates of an enemy's intentions and capabilities, but it cannot be expected to foretell the precise future operations of the enemy.

While the predominant view in the literature on intelligence failure and strategic surprise is a pessimistic one – that in the difficult job of I&W intelligence, surprise is

inevitable – scholars do not necessarily agree on any specific cause of intelligence failures. According to Betts, intelligence failures are more often due to political and psychological flaws than organizational structure.[17]Intelligence will always be less than perfect and, as history shows us, surprise can never be completely prevented. Walter Laqueur, Mark Lowenthal, Robert Jervis, and Richard Betts have attributed the main reasons why intelligence fails to tendencies that are inherent in most bureaucracies.[18]The public often blames intelligence agencies, a propensity that policymakers are happy to encourage because it shifts the responsibility away from them.[19]But whether or not the IC is unfairly or too frequently blamed for mistakes, it is important to agree on what is meant by intelligence failure.

Some argue that most intelligence failures are essentially the result of faulty analysis and/or inadequate intelligence collection, whereas others argue that failures occur either because policy consumers disregard or misinterpret the intelligence reporting they received.[20]Mark Lowenthal provides a good elucidation of faulty analysis: "An intelligence failure is the inability of one or more parts of the intelligence process—collection, evaluation and analysis, production, dissemination—to produce timely, accurate intelligence on an issue or event of importance to national interests."[21]Meanwhile, Abram N. Shulsky offered an explanation for intelligence failure that focuses on those who receive intelligence: "A misunderstanding of the situation that leads a government (or its military forces) to take actions that are inappropriate and counterproductive to its own interests."[22]

A better definition of intelligence failure involves a combination of the two explanations, with an acknowledgement to the fact that the enemy gets a vote:

intelligence failure is the result of an adversary's actions that were not identified during the intelligence cycle and achieves strategic surprise, despite the government having all the information necessary to anticipate the events and its consequences. For example, Nigerian-born Umar Farouk AbdulMutallab, a member of an affiliated branch of al-Qaeda, tried to detonate explosives hidden in his underwear as a Northwest Airlines flight from Amsterdam, Netherlands made its approach to Detroit, Michigan on December 25, 2009. Fortunately, for reasons reportedly involving human and technical error, the attempted Christmas bombing did not succeed. In his public comments, President Obama said:

> The U.S. government had sufficient information to have uncovered this plot and potentially disrupt the Christmas Day attack, but our intelligence community failed to connect those dots, which would have placed the suspect on the no-fly list.[23]

Umar Farouq Abdulmuttalab had a multiple-entry U.S. visa. His father, a leading banker in Nigeria, warned US authorities before the attack that his son might be involved with Islamic extremists, but the information failed to prompt a response such as canceling the visa. After a scathing report on intelligence failures and failed Christmas Day bomber by the Senate Intelligence Committee, the Director of National Intelligence, Admiral Dennis Blair acknowledged in a statement "institutional and technological barriers remain that prevent seamless sharing of information."[24]In other words, the failed Christmas Day bomb attempt was an intelligence failure because an adversary's actions that were not identified during the intelligence cycle, and it almost achieved strategic surprise, despite the government having all the information necessary to anticipate the events and prevent its consequences. Finally, on the heels of a number of intelligence failures involving the Fort Hood shooter, failed Christmas Day bomber Umar Farouq

Abdulmuttalab, and questions about failed Times Square bomber Faisal Shahzad, President Obama replaced Admiral Blair as the Director of National Intelligence on May 28, 2010.

Strategic surprise, such as Pearl Harbor and 9/11 attacks, attracts the most attention from policymakers, and it is this type of intelligence failure that we will focus on. Surprise is a chronic phenomenon throughout the history of warfare. Napoléon once said, "uncertainty is the essence of war, surprise its rule."[25]The failure to detect indications of a surprise attack is by far the most widely studied subset of intelligence failure. The high incident of surprise throughout history is itself not surprising. As Richard Betts argued, “surprise is by definition impossible to foresee…If attack preparations are detected, understood, and countered, then there is no surprise.[26]

Beginning with Roberta Wohlstetter’s classic book on Pearl Harbor, scholars have attempted to determine how it can be possible that the most capable intelligence system in the world appears to be taken frequently by surprise. Thomas C. Schelling wrote the following passage about the nature of surprise in the Foreword to Roberta Wohlstetter’s book:

> Surprise, when it happens to a government, is likely to be a complicated, diffuse, bureaucratic thing . . .Surprise is everything involved in a government’s . . . failure to anticipate effectively . . . the danger is in a poverty of expectations—a routine obsession with a few dangers that may be familiar rather than likely.[27]

Roberta Wohlstetter concluded that the problem of predicting surprise attack was intractable. Wohlstetter believed that there was not too little information about Japanese intentions, but too much; US officials had to deal with too many ‘signals’ or warnings, and too much background ‘noise’, an intelligence overload combined with strong beliefs about Japanese capabilities and intentions prevented senior American ranks from

listening to the ‘right’ signals.[28]Throughout history policymakers and planners have pinned their hopes on technology to solve this problem. However, as Wohlstetter concluded, the roots of surprise lie in aspects of human perception and uncertainties too basic for technological advances to completely eliminate.[29]Uncertainty and surprise are enduring phenomena that present a particularly difficult challenge for strategic intelligence warning.

Consequences of Intelligence Failure. Accompanying this plethora of explanations for intelligence failures is an equally broad range of prescriptions for reform. The most common response to an intelligence failure has been to attempt to reorganize the IC. Over the past 65 years, since Congress passed the National Security Act of 1947, there have been more than 20 official commissions and executive branch studies that have proposed organizational and administrative adjustments to improve the operation of the IC. [30] [31]

Unfortunately, few of these commissions have provoked meaningful change, and none of the reforms have put an end to intelligence failures. The increasingly multi-polar nature of international affairs, and the ability of minor actors to have a major impact on national security, has placed a premium on the IC’s ability to reduce uncertainty, identify risks and opportunities, as well as provide actionable intelligence from the White House to the foxhole. However, simply fine-tuning the IC organizational structure is inadequate to meet current and foreseeable escalating intelligence requirements.

Regrettable as it may be, the fact is that intelligence will always be imperfect and, as history clearly demonstrates, surprise can never be completely prevented. Thus, intelligence reforms alone are unlikely to prevent future intelligence failures. Rather, a

fundamental rethinking of how the IC operates at the strategic, operational, and tactical levels is needed. Far too often we only address problems only after we have experienced significant harm. Following he attempted Christmas Day airplane bombing over Detroit, President Obama said, "time and again we've learned that quickly piecing together information and taking swift action is critical to staying one step ahead of a nimble adversary…so we have to do better, and we will do better, and we have to do it quickly."[32]So, what is the most proactive way to improve the intelligence process and mitigate intelligence failures during the unpredictable 21st century?

An Antidote for the Pathology of Intelligence Failure

The presumption of surprise and incomplete intelligence requires exhaustive research upon which to build the case for specific warning.[33]The current intelligence cycle is the never-ending process of developing raw information into reliable, accurate finished intelligence for use by the President, policymakers, military commanders, and other consumers to make educated decisions; time is always of the essence. This intelligence cycle has a wide variety of interrelated intelligence operations: planning & direction, tasking & collection, processing & exploitation, analysis & production, dissemination & integration, and evaluation & feedback.[34]However, the current intelligence cycle model has three major flaws. First, the current intelligence cycle does not take into account the relationship between targets, consumers, and producers of intelligence. Secondly, the current intelligence cycle model does not promote proactive scanning of the environment for weak signals. Thirdly, the current intelligence cycle model is not fast enough to keep up with today's priority intelligence targets (e.g. non-state actors, transnational criminal organizations, and terrorist groups), which are greater in number and are often more obscure in character. Because of this, the IC

should jettison the current intelligence cycle model for a new intelligence framework that fosters greater collaboration, integration, and initiative among its stakeholders and partners.

The Intelligence Trinity. Carl von Clausewitz's concept of the fascinating trinity deals with three interactive points of attraction (chance, primordial hatred, and reason) that are simultaneously pulling the object in different directions and forming complex interactions with each other.[35]Similarly, there is a Clausewitzian trinity at work within the IC. The intelligence trinity concept has three interactive points of attraction: Producers, Consumers, and Targets (see figure 2). The actors in the intelligence trinity are simultaneously pulling each other in different directions and forming complex interactions and reactions within a complex security environment. This inherent friction that exists within the intelligence trinity among the intelligence professional (Producer), the decision-maker he or she supports (Consumer), and the adversary who attempts to conceal its activities (Target) directly and indirectly drives intelligence. Friction among the actors in the intelligence trinity is one of the causes of intelligence failure.

Know your Adversary. The highest goal of every espionage service is the penetration of the enemy’s decision-making machinery; absent this type of access, a fundamental presumption is that the adversary usually will attempt to surprise us.[36]If he cannot or does not attempt to conceal completely what he is getting ready to do, he will of least attempt to deceive us on some aspects of his plans and preparations. Reducing uncertainty requires the IC to obtain information from an adversary who would rather keep it concealed. All countries are vulnerable to deception. For example, the Germans used active military deception to achieve surprise when they attacked Russia in 1941,

and the Israeli Army achieved surprise when they attacked Egypt in 1967. The ultimate goal of an adversary's deception stratagem is to confuse his enemy and lead him to become quite certain, very decisive, and wrong.[37]The goal of intelligence is truth, but the quest for that truth "involves a struggle with a human enemy who is fighting back."[38]

Know your Consumers. Strategic intelligence must actively support higher-level officials— policymakers and military commanders—relating to the current activities, policies and objectives of innumerable nations with whom they need to deal. Ironically, a consumer may reject or twist good intelligence because it fails to fit into their plan or preconceptions. For example, intelligence may report that the policy, to which the leader is committed, is likely to entail high costs with dubious prospects for success. Ultimately, it is not the duty of intelligence to build political support for a policy.[39]It is an axiom of intelligence that warning does not exist until it has been conveyed to the policymaker, and that he must know that he has been warned. [40]On the other hand, one of the most important things that policy officials can do to obtain the intelligence they need is simply to ask the right questions.

The External Security Environment. The IC seeks to make sense of this external environment and transform it into something more stable, certain, simple, and clear. Intelligence tradecraft will continue to get harder as the state of the world continues to become more complex and uncertain. Due to the proliferation of technology, minor state and non-state actors are now able to take actions wholly out of proportion to their size or wealth. The IC will likely encounter surprises from an adversary's use of known technology in unexpected ways and the innovative application of combinations of new technologies.[41]Given a more rapid transfer speed for all types of information, today's

strategic leaders often have less time to address situations, make plans, prepare a response, and execute for success.

Hindsight is always easier than foresight. A central theme in this paper is that intelligence reforms, which account to a reorganization, are unlikely to prevent future surprises. The author largely based this argument on the nature of the security environment in the 21st century. Owen Jacobs described the external security environment as being filled with volatility, uncertainty, complexity and ambiguity, hence the popular Army War College acronym "VUCA."[42]Building upon Jacobs' work, there are three additional descriptors that help to more accurately describe the current security environment: entropy, recursiveness, and randomness. Ironically, the new acronym formed by adding theses three new terms to VUCA, hence the acronym VERRUCA, is also a medical term for warts. The challenge for the strategic intelligence is interpreting and understanding this evolving VERRUCA environment:

> Volatility refers to the rate of change of information and the rate of change of the situation. A rapidly changing environment calls for adaptive and innovative decision-making. We must have a better way of anticipating the future. [43]
>
> Entropy refers to the degree of disorder or uncertainty in a system and describes the measure of the disorder or randomness in a closed system or society.[44]Entropy is a measure of the uncertainty, or more precisely unpredictability, associated with a random variable.
>
> Recursiveness means that the world in which we now live has an increasingly number of feedback loops, causing events to be the cause of other events.[45]Information flows and spreads swiftly, thus accelerating recursive feedback loops, and events are considered to be going "viral."
>
> Randomness means something or an event that lies outside the realm of our regular expectations and arises from forces that cannot be reduced by knowledge and analysis.[46]The future is not implied by past events; instead, it is unexpectedly created by the complexity of our current actions.

> Uncertainty stems from the inability to know everything about the current situation and the difficulty of predicting what the effects of a proposed change today will be on the future.[47]
>
> Complexity differs from uncertainty, though its effects may sometimes be similar. The web of cause and effect linkages—second, third, and multiple-order effects have become more difficult in our globalized, technologically connected world. [48]
>
> Ambiguity exists when a decision maker does not understand the significance of a given event or situation—doesn't know what is happening. Ambiguity can also occur when an event can legitimately be interpreted in more than one way.[49]

The intelligence trinity coexists within an evolving VERRUCA security environment. The external security environment presents a particularly difficult challenge for strategic intelligence warning. In today's VERRUCA environment, it is imperative that all participants exchange information expeditiously and precisely. Intelligence can help manage uncertainty, defining its scope and specifying what is known and what is likely to stay unknown. This type of knowledge helps senior policymakers determine what steps the government can take to move events in a direction favorable to the US.

The Adaptive Intelligence Framework. It is a truism that a production chain or cycle is only as strong as its weakest link. The classic intelligence cycle is neat, easily displayed, and quickly understood, but the problem is that intelligence, as practiced, doesn't really work that way. As Kristan J. Wheaton states, "the intelligence cycle, as a depiction of how the intelligence process works, is a World War II-era relic that is way past its sell-by date."[50]

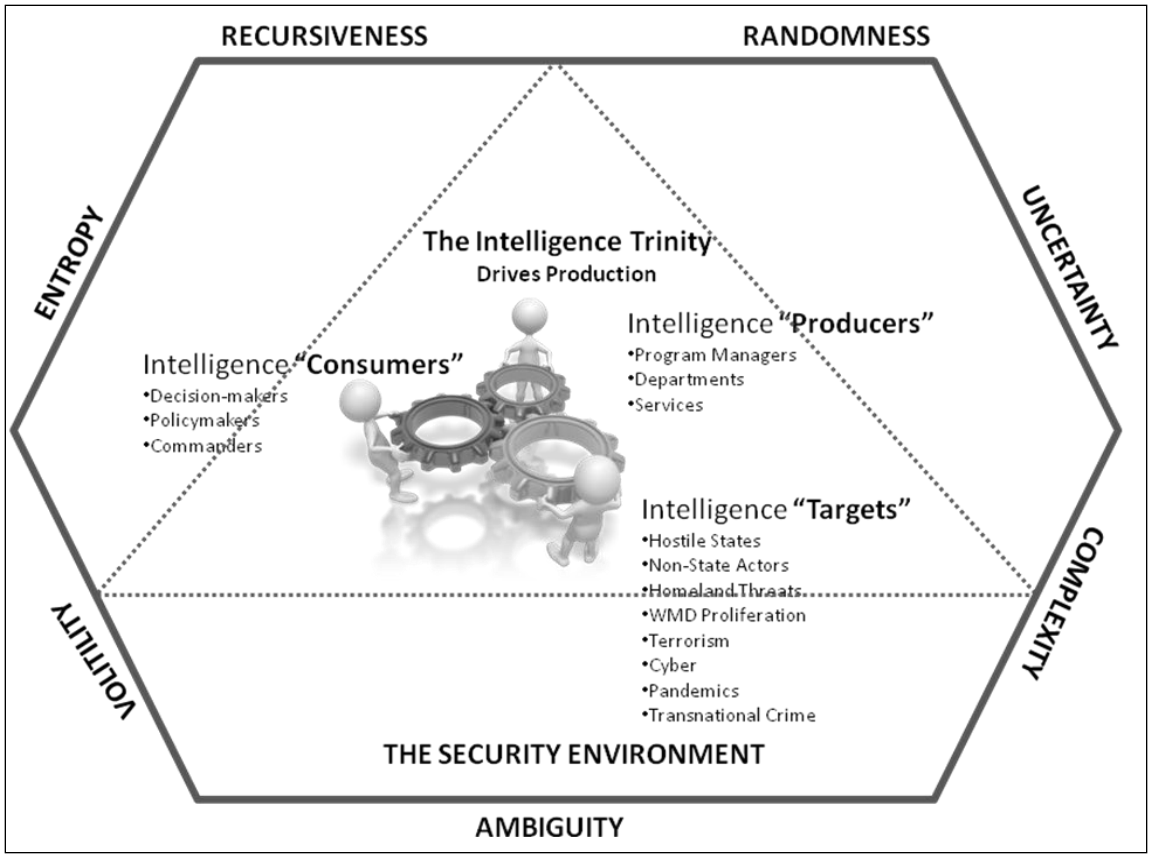

Figure 2:

In the post-9/11 world, intelligence must move faster and leverage all sources of intelligence information. A number of scholars and practitioners have attempted to rectify the problems with the intelligence cycle but none has caught on among intelligence professionals and none has been able to de-throne the intelligence cycle as the dominant image of how intelligence works. It is clear that the IC cannot operate as it has in the past. A consequent necessity is a reevaluation of the intelligence cycle to counter the threats we currently face; to adapt rapidly to these threats as they change over time; and to address new threats as they emerge.[51]

Put another way, the speed, precision and accuracy of our modern weapons systems must be equaled by the speed, precision and accuracy of our future

intelligence products. The best intelligence in the world is worthless unless it is effectively and accurately communicated to those who need it both in the non-intelligence components of the federal government, and to relevant state, local, and tribal authorities.[52]To accomplish this, a nine-step dynamic and never-ending intelligence framework is needed to replace and improve upon the fundamental vision of the current five-step intelligence cycle model. The adaptive intelligence framework will not be a panacea for all existing IC problems. The steps are:

> **1. Scanning:** Self-initiated, continuous process of actively searching the environment for and listen to weak signals that indicate change. Constant scanning is conducted for each of the other eight steps individually and for the Intelligence Cycle as a whole. The key is the first step—awareness of the anomaly.
>
> **2. Planning and Direction:** Deciding what is to be monitored and analyzed. Direction usually comes from the decision makers that the intelligence activity supports. Customers must be involved in creating products, as well as assessing their value.
>
> **3. Collection:** The obtaining of raw information using a variety of collection disciplines. It is important to understand that information from collection sources is information, not intelligence. Raw information is often incomplete or, taken out of context or without understanding its origin and purpose, possibly misleading.
>
> **4. Processing and Exploitation:** Refining and synthesis of the raw information into a form intelligence analysts can use. This is done through a variety of methods including decryption, language translation, and data reduction. Processing includes the entering of raw data into databases where it can be exploited for use in the analysis process.
>
> **5. Collaboration and Integration:** Collaboration and integration is core to any modern description of the intelligence process. Discovery of all information allows the uncovering of information having a relationship to other data, providing a better opportunity to “connect the dots.” We must synchronize collection, analysis, and counterintelligence so that they are fused—effectively operating as one team.
>
> **6. Analysis and Production:** The data that have been processed are translated into a finished intelligence product, which includes integrating, collating, evaluating and analyzing what it all means. An incorrect

interpretation of the data may or may not be a direct result of enemy intentions.

7. Information Sharing: Intelligence agencies have moved from a "need to know" culture to a "need to share" approach recommended by the 9/11 Commission. Information sharing behavior is “responsibility to provide” mindset to exchange intelligence information between collectors, analysts, and consumers. Simultaneously, consumers must protect the information made available to them.

8. Dissemination: Providing the results of processing to consumers, including consumers in the IC. These intelligence products will enable decision-makers and commanders to make better decisions faster than an adversary. The goal of dissemination is simple, get the information that is relevant to the decision maker in a timely fashion while being accurate. The consumer may ask additional questions and the intelligence cycle begins again.

9. Evaluation: The evaluation step shifts the focus of the process from the intelligence analyst to the decision-maker. Decision-making can start once the threats and opportunities for change have been identified. Options are discussed as to what actions, if any, must be taken to solve the problem. Constant feedback (which includes soliciting feedback from consumers) is conducted for each of the other eight steps individually and for the Intelligence Cycle as a whole.[53] [54] [55]

The adaptive intelligence framework is non-sequential and continuous (see figure 3). The steps can be performed out of order or skipped if the situation dictates. Unity of effort is critical. It is the responsibility of the intelligence professional to call policymakers’ attention to dangers they seem to be overlooking or understating. Consequently, the IC must focus greater attention on high impact-low probability threats to US national security interests. These early indications of change in the VERRUCA environment may easily go unnoticed in today’s information overload; and once found, it can still elude traditional inductive and deductive analytical reasoning.

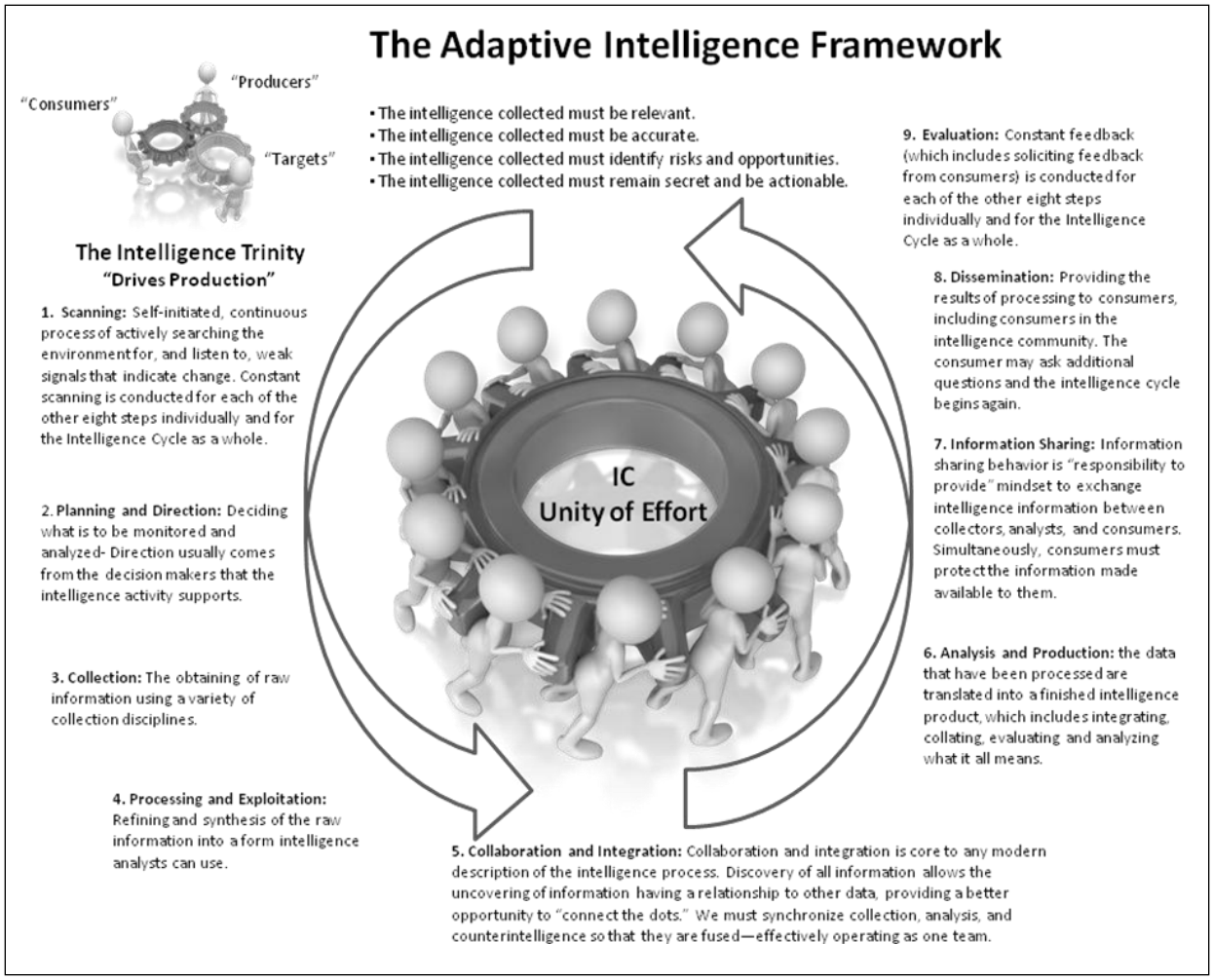

Figure 3:

In the 21st century, the ability to produce, share, and leverage intelligence will replace the ownership and/or control of assets as a primary source of competitive advantage. The IC must adapt to the ever-changing VERRUCA environment and evolving hybrid threat. Adaptability will be as important in intelligence analysis as it is to combatants on the battlefield. It is virtually impossible to have complete knowledge about all of the factors governing strategic decisions; hence, these decisions must be made with the associated risk that incomplete understanding brings.

One of the most enduring and influential forces in warfare is uncertainty, which is the same as Clausewitz's famous "fog of war." Intelligence is about reducing uncertainty— most intelligence failures were the result of systemic weaknesses in the way the IC collects, analyzes, and disseminates intelligence. Intelligence can distinguish true uncertainty from simple ignorance by systematically assembling all available information, but it cannot eliminate uncertainty and it cannot prevent all surprises, including some big ones.[56]The IC must take care that it does not lose sight of what warning really is: the considered judgment of the finest analytic minds available, based on an exhaustive and objective review of all available indications, which is conveyed to the policy official in sufficiently convincing language that he is persuaded of its validity and takes appropriate action to protect the national interest.[57]

Conclusion

It is appropriate to end by restating that intelligence will always be imperfect and, as history demonstrates, surprise can never be completely prevented. The IC is composed of 17 fiercely independent agencies, and many of the legacy bureaucratic problems within the IC place it at greater risk of being consistently unable to make decisions or take actions faster than its opponents. Necessarily, to be effective, the IC must adapt. To accomplish this adaptation, a nine-step dynamic and never-ending intelligence framework is needed to replace and improve upon the current five-step intelligence cycle model. The adaptive intelligence framework proposed in this paper is an enabler for better intelligence; however, it is not a silver bullet. The remedy, however, does require US intelligence agencies to overcome ingrained resistance to change. The nation should not wait for another commission in the aftermath of another intelligence failure to force widespread change in the IC.

The future is neither inevitable nor immutable. The IC has become used to being blamed for things for which it was not responsible and which it could not conceivably have predicted. Unfortunately, as the U.S. has been surprised in the past, it shall be surprised again in the future. As the world changes, the single most important requirement for the IC is to change with it. Most intelligence failures occur when intelligence agencies prove unable to disseminate the right information to the right decision makers at the right time. In the post-9/11 world, intelligence must move faster and leverage all sources of intelligence against an adversary.

Knowledge in advance enables one to be prepared, as described in the Latin proverb *Praemonitus, praemunitus*, which loosely translates as forewarned is forearmed. The object of intelligence is to inform our decisions and make better choices. However, even the best analytical practices will sometimes result in assessments that later prove inaccurate.[58]John Keegan concludes in his book Intelligence in War that intelligence, however good, is not necessarily the means to victory; that, ultimately, it is force, not fraud or forethought, that counts.[59]In other words, intelligence is an enabler, which should establish the grounds for a decision advantage over a belligerent.

Any impressions that an adaptive intelligence framework is the perfect panacea are false. The adaptive intelligence framework is just another step toward a vision of a more perfect IC. Anticipation of the consumer's needs and adversary's likely course of action on the various envisioned battlefields are steps toward providing better intelligence support. The adaptive intelligence framework provides another tool to assist the analyst to think about the strategic VERRUCA environment. The ideas that have been argued here are intended to contribute to a constructive dialogue on such change.

The author of this paper recognizes how difficult it is to establish a new way of doing business. Arguably the most powerful factor that causes any doctrine to change is a change in the strategic objectives of the nation brought about by changes in the strategic environment. The IC must be both adaptable and flexible in the face of new external threats and inevitable internal change. In the words of Louis Pasteur, "chance favors the prepared mind."[60]

Endnotes

[1] United States Congress, Intelligence Reform and Terrorism Prevention Act of 2004, 108th Congress, 2nd Session, January 20, 2004.

[2] Linked from Intelligence Home Page, http://www.intelligence.gov/about-the-intelligence-community/, (accessed October 28, 2011).

The 17 IC member agencies are: Air Force Intelligence; Army Intelligence; Central Intelligence Agency; Coast Guard Intelligence; Defense Intelligence Agency; Department of Energy; Department of Homeland Security; Department of State Department of the Treasury; Drug Enforcement Administration; Federal Bureau of Investigation; Marine Corps Intelligence; National Geospatial-Intelligence Agency; National Reconnaissance Office; National Security Agency; Navy Intelligence; and the Office of the Director of National Intelligence.

[3] Commission on Intelligence, An Intelligence Community Primer, linked from The Global Security Home Page, http://www.globalsecurity.org/intell/library/reports/2005/wmd_report_25mar2005_appdx-c.htm (accessed December 6, 2011).

[4] James Clapper, "Remarks and Q & A by Director of National Intelligence Mr. James Clapper," Bipartisan Policy Center (BPC) — The State of Domestic Intelligence Reform, 6 October 2010, http://www.dni.gov/speeches/20101006_speech_clapper.pdf, (accessed December 9, 2011).

[5] Richard K. Betts, "Fixing Intelligence," *Foreign Affairs*, Vol. 81, (January/February 2002): 44.

[6] Walter Laqueur, *A World of Secrets: The Uses and Limits of Intelligence* (New York, NY: Basic Books, 1985), 8.

[7] Stephen A. Cambone, "The National Security Act of 1947– 26 July 1947." *A New Structure for National Security Policy Planning* (Washington, DC: CSIS, 1998), 228-32.

[8] David T. Moore, *Critical Thinking and Intelligence Analysis*, Occasional Paper Number Fourteen (Washington, DC: National Defense Intelligence College, 2006), 2.

[9] Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02, (Washington, DC: The Joint Staff, April 12, 2001), 208.

The Joint Chiefs of Staff's Dictionary of Military and Associated Terms defines intelligence as:

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.

[10] The Clark Task Force, of the Hoover Commission in 1955, defined intelligence as all the things that should be known in advance of initiating a course of action.

[11] Central Intelligence Agency (Office of Public Affairs), *A Consumer's Guide to Intelligence*, (Washington, DC: Central Intelligence Agency, 1999), vii.

[12] Sherman Kent, "Prospects for the National Intelligence Service," *Yale Review* 36, (Autumn 1946):117.

[13] Kent, Sherman, *Strategic Intelligence for American World Policy*. (Princeton, NJ: Princeton University Press, 1949), 5-25.

[14] Abram N. Shulsky (revised by Gary J. Schmitt), *Silent Warfare: Understanding the World of Intelligence* (Washington, DC: Brassey's (US), 2002 [third edition]), 1-3, 171-176.

[15] Richard K. Betts,"Analysis, War, and Decision: Why Intelligence Failures Are Inevitable." *World Politics* 31, (Winter 1978), 88.

[16] Joseph S. Nye, Jr., "Peering into the Future," *Foreign Affairs* (July/August 1994): 88.

[17] Richard K. Betts, "Analysis, War and Decision: Why Intelligence Failures are Inevitable", *World Politics* Vol. 31, (1978-1979), 67.

[18] Laqueur, 8; Lowenthal, 50; Jervis, 3-6; and Betts, 44.

[19] Robert Jervis, *Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War* (Ithaca, NY: Cornell University Press, 2010), 1.

[20] W. C. Matthias, *America's Strategic Blunders: Intelligence Analysis and National Security Policy, 1936-1991* (University Park, PA: Penn State Press, 2001); and R. J.Heuer, Jr. *Psychology of Intelligence Analysis* (Washington, DC.: CIA Center for the Study of Intelligence, 1999), 65.

[21] Mark M. Lowenthal, "The Burdensome Concept of Failure," in *Intelligence: Policy and Process,* ed. Alfred C. Maurer, Marion D. Tunstall, and James M. Keagle (Boulder, CO: Westview Press, 1985), 51.

[22] Schulsky & Schmitt, *Silent Warfare,* 63.

[23] Dan Lothian and Suzanne Malveaux, “Obama on intel system: 'This was a screw-up,'” linked from The CNN Home Page, http://www.cnn.com/2010/POLITICS/01/05/obama.terror. meeting/index.html, (accessed March 13, 2012).

[24] Jake Tapper, President Obama To Replace Director of National Intelligence Dennis Blair, linked from The ABC News Home Page, http://abcnews.go.com/blogs/politics/2010/05/exclusive -president-obama-to-replace-director-of-national-intelligence-dennis-blair/, (accessed March 12, 2012).

[25] Michael Handel, "Intelligence and the Problem of Strategic Surprise," *The Journal of Strategic Studies*, (September 1984): 270.

[26] Richard Betts, *Surprise Attack: Lessons for Defense Planning* (Washington, DC: Brookings Institute, 1982), 18.

[27] Thomas C. Schelling, Foreword to Roberta Wohlstetter, *Pearl Harbor: Warning and Decision* (Stanford, CA: Stanford University Press, 1962), iii.

[28] Roberta Wohlstetter, *Pearl Harbor: Warning and Decision* (Stanford, CA: Stanford University Press, 1962), 397.

[29] Barry D. Watts, *Clausewitzian Friction and Future War* (Washington, D.C.: National Defense University, 2004), 40.

[30] Larry C. Kindsvater, “The Need to Reorganize the Intelligence Community,” The Center for the Study of Intelligence, linked from The CIA Home Page, https://www.cia.gov/library/ center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol47no1/index.html, (accessed January 28, 2012).

[31] As early as 1949, the first Hoover Commission called for the CIA to be the “central” organization of the national intelligence system. In 1955, the second Hoover Commission recommended that the DCI concentrate on his Community responsibilities and that an “executive officer” oversee the day-to-day operations of the CIA. In 1971, the Schlesinger Report discussed creation of a DNI, but did not propose establishing such a position over the DCI. Instead, the report simply recommended that the nation needed a strong DCI who could control intelligence costs and production. In 1976, the Senate Select Committee to Study Government Operations with Respect to Intelligence Activities (the Church Committee) issued a report that, inter alia, recommended that national intelligence funding be appropriated to the DCI, thereby giving him control over the entire IC budget. The report also recommended separating the DCI from the CIA. In 1992, proposed legislation from Senator Boren and Representative McCurdy called for a DNI with programming and reprogramming authority over the entire IC and the ability to temporarily transfer personnel among IC agencies. In 1996, the House Permanent Select Committee on Intelligence produced a staff study—IC21: The Intelligence Community in the 21st Century—that called for more corporateness across the Community and strengthened central management of the IC by providing the DCI additional administrative and resource authorities. It also proposed consolidating all technical collection activities into one large agency; refining the “center” concept as employed by the CIA; and creating two deputy DCIs, one for Analysis and one for Community Management, including collection. In 2005, the aftermath of the intelligence failure(s) that failed to prevent the terrorist attacks on 9/11, and the subsequent investigation by the 9/11 Commission, Congress legislated

and President Bush passed the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) to provide more effective threat warning. The IRTPA established the position of the Director of National Intelligence (DNI) to serve as head of the IC and act as the principal adviser to the President on intelligence matters related to national security.

[32] Dan Lothian and Suzanne Malveaux, “Obama on intel system: 'This was a screw-up,'” linked from The CNN Home Page, http://www.cnn.com/2010/POLITICS/01/05/ obama.terror.meeting/index.html, (accessed March 13, 2012).

[33] Cynthia M. Grabo, *Anticipating Surprise: Analysis for Strategic Warning,* (Washington DC: Joint Military Intelligence College, 2002), iii.

[34] Office of the Director National Intelligence, “A Dynamic Process Fueling Dynamic Solutions,” How Intelligence Works, linked from The ODNI Home Page, http://intelligence.gov/ about-the-intelligence-community/how-intelligence-works/, (accessed February 14, 2012).

[35] Carl von Clausewitz, *On War, ed. and trans.*, Michael Howard and Peter Paret. (Princeton: Princeton University Press, 1976), 119-120.

[36] Grabo, *Anticipating Surprise: Analysis for Strategic Warning*, 36.

[37] Barton Whaley, *Stratagem: Deception and Surprise in War* (Cambridge, MA: Massachusetts Institute of Technology, 1969), 177-178.

[38] Schulsky & Schmitt, *Silent Warfare,* 1-3.

[39] Ibid.

[40] Ibid.

[41] Aris A Pappas and James M. Simon, Jr., “The Intelligence Community: 2001-2015,” The Center for the Study of Intelligence, linked from The CIA Home Page, https://www.cia.gov/ library/center-for-the-study-of-intelligence/csi-publications/csistudies/studies/vol46no1 /article05.html, (accessed January 28, 2012).

[42] T. Owen Jacobs, *Strategic Leadership: The Competitive Edge* (Fort Leslie J. McNair, Washington, D.C.: Industrial College of the Armed Forces, 2000), 24.

[43] Ibid., 24.

[44] Merriam Webster website, linked from The Merriam Webster Home Page, http://www.merriam-webster.com/dictionary/entropy, (accessed February 20, 2012).

[45] Nassim Nicholas Taleb, *The Black Swan* (New York, NY: Random House, 2010), xxvi.

[46] Ibid., xxii.

[47] Jacobs, *Strategic Leadership: The Competitive Edge,* 24.

[48] Ibid.

[49] Ibid.

[50] Kristan J. Wheaton, Sources and Methods, linked from The Sources and Methods Home Page, http://sourcesandmethods.blogspot.com/2011/05/lets-kill-intelligence-cycle-original.html, (accessed February 14, 2012).

[51] Intelligence Community Information Sharing Strategy, linked from The ODNI Home Page, http://www.dni.gov/reports/IC_Information_Sharing_Strategy.pdf, (accessed February 19, 2012).

[52] The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, Report to the President of the United States, March 31, 2005, 26.

[53] Central Intelligence Agency, "The Intelligence Cycle," Who We Are & What We Do, linked from The CIA Home Page, https://www.cia.gov/kids-page/6-12th-grade/who-we-are-what-we-do/the-intelligence-cycle.html, (accessed February 14, 2012).

[54] U.S. National Intelligence: An Overview 2011, linked from The ODNI Home Page, http://www.dni.gov/IC_Consumers_Guide_2011.pdf, (accessed 19 February 19, 2012).

[55] Intelligence Community Information Sharing Strategy, linked from The ODNI Home Page, http://www.dni.gov/reports/IC_Information_Sharing_Strategy.pdf, (accessed February 19, 2012).

[56] Paul R. Pillar, "Think Again: Intelligence," *Foreign Policy*, (January-February, 2012): 15.

[57] Grabo, *Anticipating Surprise: Analysis for Strategic Warning*, 169.

[58] A Tradecraft Primer Structured Analytic Techniques for Improving Intelligence, linked from The DocStoc Page, http://www.docstoc.com/docs/5982545/A-Tradecraft-Primer-Structured-Analytic-Techniques-for-Improving-Intelligence, (accessed February 18, 2012).

[59] John Keegan, *Intelligence in War; Knowledge of the Enemy from Napoleon to Al-Qaeda* (New York: Alfred A. Knoph, 2003), 334.

[60] Grabo, *Anticipating Surprise: Analysis for Strategic Warning*, 39.