Strategy Research Project

SYSTEMS ANALYSIS, CENTERS OF GRAVITY AND HOMELAND SECURITY

BY

LIEUTENANT COLONEL DAVID RODRIGUEZ
United States Air Force

USAWC CLASS OF 2011

U.S. Army War College, Carlisle Barracks, PA 17013-5050

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle State 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 *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
25-02-2011	Strategy Research Project	

4. TITLE AND SUBTITLE

Systems Analysis, Centers of Gravity and Homeland Security

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Lieutenant Colonel David Rodriguez

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

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

Professor Frank L. Jones
Department of National Security and Strategy

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

Since the terrorist attack of September 11, 2001, the Department of Homeland Security (DHS) has aggressively instituted a broad set of security procedures to protect the American people. These security measures provide multiple layers of protection using the capabilities of the federal, state and local governments. Nonetheless, the war fighting posture of the United States, the techniques utilized for achieving success in campaign planning, can be adapted to provide some measure of increased benefit in defense of the homeland. By identifying the U.S. strategic centers of gravity (COGs) and incorporating a comprehensive systems assessment, a useful framework can be added to the existing DHS toolkit. This paper discusses the traditional COG concept, incorporates a systems understanding of COGs and then examines the existing methodology utilized by the DHS for risk assessment. John Warden's Five Ring Model can be effectively used as a viable framework to assist in a more comprehensive risk assessment methodology by DHS. Finally, a hypothetical scenario is discussed to illustrate the usefulness of systems thinking to homeland security.

15. SUBJECT TERMS

Center of Gravity, Risk, Threat, Infrastructure, Systems

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

SYSTEMS ANALYSIS, CENTERS OF GRAVITY AND HOMELAND SECURITY

by

Lieutenant Colonel David Rodriguez
United States Air Force

Professor Frank L. Jones
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: Lieutenant Colonel David Rodriguez

TITLE: Systems Analysis, Centers of Gravity and Homeland Security

FORMAT: Strategy Research Project

DATE: 25 February 2011 WORD COUNT: 5,868 PAGES: 32

KEY TERMS: Center of Gravity, Risk, Threat, Infrastructure, Systems

CLASSIFICATION: Unclassified

Since the terrorist attack of September 11, 2001, the Department of Homeland Security (DHS) has aggressively instituted a broad set of security procedures to protect the American people. These security measures provide multiple layers of protection using the capabilities of the federal, state and local governments. Nonetheless, the war fighting posture of the United States, the techniques utilized for achieving success in campaign planning, can be adapted to provide some measure of increased benefit in defense of the homeland. By identifying the U.S. strategic centers of gravity (COGs) and incorporating a comprehensive systems assessment, a useful framework can be added to the existing DHS toolkit. This paper discusses the traditional COG concept, incorporates a systems understanding of COGs and then examines the existing methodology utilized by the DHS for risk assessment. John Warden's Five Ring Model can be effectively used as a viable framework to assist in a more comprehensive risk assessment methodology by DHS. Finally, a hypothetical scenario is discussed to illustrate the usefulness of systems thinking to homeland security.

SYSTEMS ANALYSIS, CENTERS OF GRAVITY AND HOMELAND SECURITY

Since the terrorist attack on September 11, 2001, there have been more than 30 different terrorist plots foiled by the combined efforts of the United States (U.S.) federal, state and local governments.[1] Al Qaeda's recently foiled attempt (November 2010) utilizing cargo bombs aboard United Parcel Service (UPS) cargo planes illustrates their continued intent to attack U.S. interests and an increasing sophistication in the terrorist group's targeting methodology.[2]

An analysis of Al Qaeda's foiled plots reveals a wide array of targets to include bridges, major financial institutions, the New York Stock Exchange and various critical infrastructure assets.[3] The Department of Homeland Security (DHS) in an effort to provide security in such an uncertain environment, has aggressively instituted a broad set of security procedures aimed at providing multiple layers of protection using the capabilities of the federal, state and local governments. Nonetheless, despite DHS success in quickly establishing a robust program, improvements are still necessary.

The United States Government (USG) has adopted a war fighting posture in the battle against terrorism and consequently, the techniques utilized for achieving success in traditional campaign planning can be adapted to provide a useful mechanism for improving the nation's security. By identifying the U.S. strategic centers of gravity (COGs) and incorporating a comprehensive systems assessment, a useful framework can be added to the existing DHS toolkit for identifying critical targets and conducting comprehensive analysis of the risk posed by terrorist groups such as Al Qaeda.[4]

This paper reviews the traditional center of gravity concept as espoused in the Joint Publication 5.0, *Joint Operational Planning*, and then examines Colonel John A.

Warden III's theory (Five Ring Model) of viewing the enemy as a system. Next, the existing methodology utilized by the DHS for critical infrastructure protection will be reviewed, followed by a discussion of how adaptation of Warden's Five Ring Model can be used as a viable framework to assist in a more comprehensive risk assessment methodology. Finally, a hypothetical scenario will be offered to illustrate the value of systems thinking in homeland security.

A Persistent Terrorist Threat

Although the security measures the United States Government (USG) installed following the September 11, 2001 attack have been successful in protecting the United States from subsequent attacks, it is not altogether clear that the existing methodology adopted by the Department of Homeland Security (DHS) is sufficiently forward looking regarding new and emerging threats.[5] The most recent National Intelligence Estimate continues to identify Al Qaeda and its affiliates as a persistent threat against the U.S. and its interests.[6] Since September 11, 2001, the panoply of security measures instituted were a reaction to an existing and known threat, but Al Qaeda has continued to adapt and evolve while still being able to recruit new members worldwide.[7]

Department of Homeland Security (DHS) Secretary Janet Napolitano has publicly articulated in a DHS report her belief in an increasing homegrown terrorist threat to include returning U.S. veterans, which if accurate, poses an even more difficult security challenge.[8] In either case, the reported threat from both external and internal terrorist groups continues to pose a serious challenge to DHS security planners. Within this context of a persistent threat from terrorist groups and the increasing attempts by terrorists to cause death and destruction in recent years, prudence dictates planners conduct a comprehensive review of existing security measures. Germain Difo, an

analyst for the American Security Project, argues now is the time to determine which methods have been effective, which methods are too costly, and the best way to adapt and prepare for the future.[9] Given the size and complexity of the political, economic, military and social systems in the United States, the potential targets are virtually endless. Consequently, not every target can be protected with limited resources, forcing leaders to make hard choices concerning risk management.[10] Security planners need to adopt a methodology that produces a security structure that is not only cost effective and sustainable in the long term, but also one that can be justified to the public.[11]

Traditional Center of Gravity Analysis

When developing a comprehensive strategy to protect the U.S. homeland, planners should consider security planning synonymous to military campaign planning. In military planning, joint doctrine requires commanders and their staff to identify and analyze adversary centers of gravity (COGs).[12] A center of gravity (COG) is defined as: "a source of power that provides moral or physical strength, freedom of action or will to act. It's what the Prussian theorist Carl von Clausewitz called 'the hub of all power and movement, on which everything depends.'"[13] One can reason that if it is good practice to identify and analyze an adversary's COGs, then it should also be good practice to analyze one's own COGs. In fact, joint doctrine specifically requires that when conducting campaign planning, the commander identify not only adversary COGs, but also friendly COGs.[14] It is this process of identifying COGs that serves as a foundation for identifying sources of power as well as sources of critical vulnerability.[15]

Adapting this COG concept to the United States for homeland security is not necessarily intuitive, however it would provide policy makers with a better understanding

of the nation's power centers and apply protective resources accordingly.[16] In attempting to adapt this COG concept to the context of homeland security, one must remember that Clausewitz envisioned the enemy acting as one single entity and that by overcoming an enemy's COG, they would then collapse completely.[17] Planners must determine how the United States acts as one entity and then specifically identify the one decisive COG that once overcome, would cause the United States to collapse. Since the United States as a whole is a very complex entity in terms of governance, economic systems, military forces and national infrastructure, one has a very difficult time attempting to identify one decisive point. It is precisely at this stage in the planning process that the traditional COG framework becomes seemingly difficult to adapt for homeland security and one may be tempted to abandon further efforts. Nonetheless, Clausewitz's theory of COG when properly applied using the enemy as a whole, or system, is still valid and applicable.[18]

Using Systems Analysis in COG Determination

This principle of understanding the enemy as a whole, or as a system, is the key to making the COG concept a useful tool for homeland security planners. In the case of the United States, a country composed of numerous complex systems, a more refined application of Clausewitz's COG theory is needed. Colonel John Warden's theory of viewing the "enemy as a system" and associated Five Ring Model used during the Desert Storm air campaign is a useful tool in the homeland security environment. Warden advocates that when thinking strategically, one must think of the enemy as a "system composed of numerous subsystems."[19] On initial consideration, one might argue using Warden's enemy as a system concept for COG determination in the United States does not apply since the situations encountered by the DHS are not the same as

Desert Storm. After all, Warden's Five Ring Model was the concept used for a massive aerial bombing campaign and not necessarily applicable when dealing with a group like Al Qaeda that does not possess an air force. However, the utility of the Five Ring Model in determining critical targets is not dependent upon the method of ordnance delivery but rather the targets attacked.

Warden's Five Ring Model is based upon the premise that all human organizations including societies are designed similarly and share certain characteristics.[20] Warden asserts these organizations all share a leadership function, an organic essential or function that converts energy in some form; an infrastructure; a population and a defensive system of some form.[21] Graphically, these shared characteristics of a system are depicted as Warden's Five Ring Model in Figure 1.

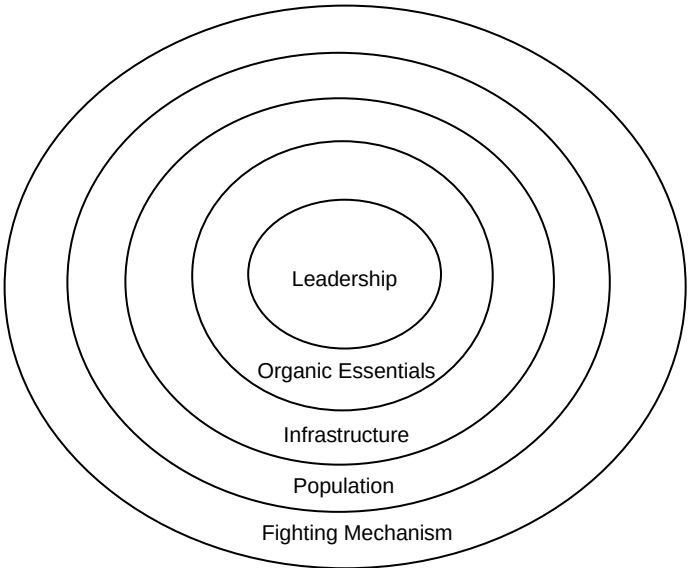

Figure 1

Warden configured his base Five Ring Model to apply to any country by identifying the applicable system components in each ring. For leadership, the obvious component is the existing government of that country; the organic essentials would be

composed of power production facilities such as electrical grids, nuclear power plants, and infrastructure correlating to bridges, railways or other key assets.[22] Warden also adapted his base model for a non-state actor such as a drug cartel, where the organic essential is changed from a traditional concept like a power plant to a drug processing center or laboratory and its associated infrastructure as its distribution network.[23] Using this adaptable Five Ring Model, a useful framework for identifying U.S. key centers of gravity emerges and more specifically, a potential framework for identifying critical vulnerabilities as well.[24]

In addition to proposing the basics tenets of the Five Ring Model, Warden and other air power theorists also advocated the concepts of strategic paralysis and parallel war. The concept of strategic paralysis is based upon an understanding of an entity as a system, composed of the five rings, where those specific parts of the system that are controlled externally and results in the system as a whole being unable to act as it wishes, or in other words, is paralyzed.[25] To achieve strategic paralysis, parallel warfare is utilized, where each major system component in each of the five rings is brought under simultaneous or near-simultaneous attack.[26] These concepts of parallel war and strategic paralysis were combined during the Desert Storm air campaign and were arguably successful in achieving the desired effect.[27]

However, in the realm of homeland security, anticipation of an aerial bombardment like the one conducted by the largest coalition of attacking forces in modern history is not likely. Nonetheless, the systems analysis methodology, the Five Ring Model, and the concept of parallel attack can be useful in refining existing homeland security strategy. When utilizing these elements, it is absolutely critical to

understand the United States as an entire system, composed of various subsystems.[28] Particularly for a complex entity like the United States, identifying COGs is rather difficult since multiple COGs will exist and they all have an interrelated impact, making it difficult to isolate one decisive point.[29] As a result of the interrelated connectivity and complexity of the U.S. homeland, terrorist attacks should not be analyzed in isolation but rather they should be analyzed in relation to the entire system and pertinent subsystems.

In conventional offensive military operations, control or damage to enough systems at the operational level can paralyze an adversary at the strategic level, without destroying the entire system.[30] In the context of terrorist attacks, one can conceive of a purposeful design to achieve a particular effect on a system rather than simple destruction of a target or the direct and immediate consequences resulting therefore.[31] For instance, if there was a terrorist attack on the port in Long Beach, California, could the port be effectively shut down for an extended period of time without being totally destroyed? If this effect were achieved, the total economic impact would be dramatically more significant than simply the physical destruction or loss of life during the attack. The effects of such an attack would ripple through the shipping sector and any associated manufacturing sector negatively affected by a stopped or slowed exchange of goods. But what if such a terrorist attack were combined with other attacks that were nearly simultaneous, designed to disrupt various subsystems that support the U.S. economic system?

Using a systems approach provides a more complete understanding by examining the impact of the attacks on the entire economic system, not in isolation or

limited to a particular sector like shipping. Attackers can exploit the initiative by incorporating the concept of parallel war, across three dimensions: time, space and the various levels of security to include local, state and federal.[32] Defending against the threat of potential, sequenced terrorist attacks requires the same measures as defending against parallel war. These measures include the identification of the enemy's real target and better coordination of all our military, law enforcement, political and economic actors to develop a comprehensive and integrated defensive strategy.[33]

Current Homeland Defense Security Protection Plan

Armed with an understanding of a systems framework in COG determination, it is also helpful to understand current homeland security policies, strategies, and plans. From the outset of its existence, the DHS utilized a broad-based approach that sought to increase security awareness by making decisions about priorities that were based upon consequences, most importantly, the impact on the American population.[34] In 2006, then DHS Secretary Michael Chertoff directed utilization of a risk-based approach in making resource allocation decisions.[35] Even with a greater emphasis on risk analysis, developing adequate security measures still presented a formidable challenge in comparing threats across so many targets as well as determining accurate consequences of a potential attack.[36]

When attempting to make risk-informed decisions, there is no certain and correct method available to measure risk accurately and completely.[37] The Rand Corporation published a report in 2005 espousing a method of risk analysis that defined risk as a function of three components: threat, vulnerability and consequence.[38] Mathematically, the RAND model of component of risk is represented as: R(Risk) = T(Threat) x V(Vulnerability) x C(Consequences). This construct provides a coherent method for

applying an analytical approach in establishing security measures. Given a near infinite number of possible terrorist targets, some mechanism to identify risk and allocate resources must be used.[39] Using RAND risk framework, one can analyze each of the variables of risk to determine the overall level of risk. For instance, if the threat to a particular target has a high probability, then the level of risk is greatly increased. Additionally, the vulnerability of the target and the consequence of the target being destroyed factor into the calculation. Unfortunately, determining the actual level of threat, or more accurately, determining the probability of an attack is difficult and often unreliable.

Intuitively, if the probability of an attack is zero, then the corresponding risk is zero. Additionally, if the consequence of the total destruction of the target is zero, then the corresponding risk is zero. More often than not however, the true risk to a target is somewhere between the extremes and deriving values for each individual risk variable is not simple. As a result, scholars in the security field such as John Mueller from the Ohio State University, argue for security measures that overlap across the broadest potential target set possible because there is a great deal of uncertainty and variability in the component risk variables.[40] The Department of Homeland Security has to some extent, adopted this same approach. Beginning with the Clinton Administration and its Presidential Decision Directive (PDD)-63, the protection of key infrastructure components essential to the nation was specifically designed to prevent and minimize any significant disruptions in services.[41] This was further refined by the Bush Administration in 2003 with the Homeland Security Presidential Directive (HSPD)-7, where the U.S. policy was to include protection of U.S. critical infrastructure and key

resources “from terrorist attacks.”[42] The resulting National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (CIKA) underscored the need to develop a “comprehensive, prioritized assessment of facilities, systems and functions” for the entire nation.[43]

The Congressional Research Service (CRS) conducted a recent review of U.S. infrastructure protection measures and identified the efforts of the DHS to protect various sectors to include public health, shipping, agriculture as well as chemical facilities.[44] The CRS concluded that as a matter of policy, federal efforts should be focused toward those targets that posed the greatest risks.[45] Although seemingly obvious, previous policy documents such as the PDD-63 or HSPD-7 contained virtually no instruction regarding the incorporation of risk. Nonetheless, the basic dilemma of correctly identifying risk based on the uncertainty and variability of factors is unknowable and makes prioritization of resources difficult. Since risk measurement for homeland security is not in the same class as auto accidents derived from reliable statistical data, determining how much to spend on protecting a potential target is still a daunting task.[46]

So how much should the taxpayer be willing to pay to mitigate risk on potential terrorist targets, especially when the probability of an attack is widely variable?[47] Reportedly, the DHS spent 34% of its budget on lowering the vulnerability of potential targets.[48] In the DHS risk analysis equation of R(Risk) = T(Threat) x V(Vulnerability) x C(Consequence), the DHS has, in essence, opted to reduce the one variable it can quantifiably control, the vulnerability variable (V). The risk analysis methodology employed in practice in essence becomes: R = V x C. Hence, some security analysts

argue that security measures should have a “dual or collateral benefit” where vulnerability across a broad group of targets is reduced.[49] Another school of thought in the security community advocates focusing on the worst case scenario where the emphasis is placed on the consequences of an attack.[50] According to the Congressional Research Service (CRS), existing risk analysis by the DHS places an assessment of target vulnerability and consequences of an attack on an 80 point scale and then adds it to the probability of an attack on a 20 point scale ($R = V \times C + V$).[51] In this manner, since the factors of vulnerability and consequence are added to the threat component, the threat or probability of an attack on a specific target is still accounted for but given significantly less weight. Taken to the extreme, the threat factor (T) to a target can be zero, but the assigned risk factor can still considered relatively high, leading policy makers to allocate resources to protect it.

The most recent National Infrastructure Protection Plan (NIPP) released in 2009 champions the utilization of a risk analysis that combines the factor of threat, vulnerability and consequence information as a function where $R = f(C,V,T)$.[52] In fact, the new NIPP significantly expanded the discussion of risk analysis and advocated the use of cross sector analysis to measure impacts across various critical infrastructure sectors.[53] While these modifications by DHS in its methodology more closely approach a comprehensive systems approach, it still falls short. For instance, the updated plan is still focused on an “asset, system, network or functional basis, depending upon the fundamental characteristic of the individual sectors.”[54] As a result, this approach does not begin at the highest level, starting with the nation as a whole system or with the economic system as an integrated whole, composed of numerous sectors. The current

DHS plan allows for systems consideration but only specifies sector systems such as communications and informational technology systems, indicating that the strategy still does not consider an assessment of the entire economic system and is limited to particular infrastructure subsystems.[55]

This methodological limitation manifests itself in the assessment of risk by not accounting fully for the potential consequence of attacks or parallel attacks. The NIPP divides consequence analysis into categories of population impact, economic impact, and psychological impact as well as governance impacts.[56] Specifically, the economic consequences are calculated based upon damage to infrastructure with respect to physical asset destruction, with a focus on the "cost to rebuild asset, cost to respond to and recover from an attack, downstream costs resulting from disruption of product or service…."[57] This construct does not incorporate any possible synergistic effects resulting from parallel, system-designed attacks aimed at a higher, national level effect, such as the overall economy of the United States. Even the fifteen National Planning Scenarios call for a governmental response that deals with the impacts of a specific type of attack.[58] None of the published scenarios contain a methodology where shocks are combined in multiple, cross attack scenarios to obtain a desired effect on a national system such as the American economy. Even if multiple, simultaneous natural disasters are assumed to be rare, this does not account for a combined natural disaster and one or more terrorist attacks. DHS acknowledges in its most recent NIPP that "nearly all sectors share relationships with elements of the energy, information technology, communications, banking and finance, and transportation sectors," but it

still does not directly discuss how to consider or measure sector impact on the overall economic system.[59]

Additionally, the U.S. Government established the National Infrastructure Simulation and Analysis Center (NISAC) to provide advance modeling of simulated attacks and provide data on their associated impacts on the nations critical infrastructure, measured in terms of their "dependencies and interdependencies," but there is no indication the focus rises above the infrastructure asset itself to the overall economic system of the nation.[60] The initial National Asset Database last updated in 2006 had more than 77,000 entries of key national assets identified for some measure of protection.[61]

Lastly, the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets acknowledges terrorists "may choose to target critical infrastructure and key assets as low-risk means to generate mass casualties, shock and panic."[62] However, what is not addressed is that terrorists may also choose to attack critical infrastructure targets and key assets for a broader, more strategic effect. Terrorists may choose to attack a national Center of Gravity (COG) such as the U.S. economic system, and terrorists may use a systems approach combined with parallel attacks. Thus far, neither U.S. Government policy nor security planning seems to incorporate a comprehensive systems approach.

Indicators of Growing Al Qaeda Sophistication

The current conventional wisdom concerning Al Qaeda's targeting indicates a propensity to select targets with a high population density to achieve a desired effect, cause disruption and display a symbolic consequence.[63] But will this existing propensity always be the standard? Since it is also commonly understood that the attack of

September 11, 2001, were highly sophisticated and involved numerous targets, attacked nearly simultaneously, why should one reasonably expect Al Qaeda to continue using the same targeting methodology? Al Qaeda has already demonstrated a willingness to conduct extensive research and pursue creative operational capabilities such as learning to pilot commercial aircraft.[64] When considering future attacks by Al Qaeda, the National Security Council has reported Al Qaeda is aggressively pursuing weapons of mass destruction (WMD) such as nuclear devices or chemical and biological agents.[65] If Al Qaeda is successful in employing weapons of mass destruction, then the previous targeting methodology is not necessarily limited or necessarily required. Although the U.S. Government has fielded a more robust system of security since the September 11, 2001 attack, utilizing a systems framework can assist in anticipating Al Qaeda targeting.

On what basis should we expect Al Qaeda targeting to diverge from traditional high population, maximum disruption targets? The U.S. Secret Service has conducted research revealing that when conducting threat assessments, "all targeted violence is the result of an understandable and often discernable process of thinking and behavior."[66] Additionally, the Secret Service discovered that individuals who committed acts of targeted violence also demonstrated a pattern of certain behavior before the event.[67] A review of foiled Al Qaeda attacks and plans has shown methods that include assassination attempts on governmental officials, attacks on infrastructure to include nuclear power plants, financial centers, refineries and even military bases.[68] Al Qaeda also exhibited these behaviors to included communication about specific organizational intent.[69]

In a review of public Al Qaeda communications, security officials acknowledge that Al Qaeda has designs on "crippling our economy" but these same officials boldly claim "no enemy of the U.S. should think a city or region can be put out of business."[70] However, a survey of existing literature on the intentions and designs of Al Qaeda reveals a "coherent long-term strategy" depicting the organizational struggle in terms of "economic war."[71] More striking is Abu-'Ubayd al-Qurashi's claim, a jihadist leader and aide to Osama bin Laden, who declared, "It is clearly apparent that the American economy is America's center of gravity…aborting the American economy is not an unattainable dream."[72] What is particularly striking is not just the emphasis on the U.S. economy as the target, but rather the terminology used: "Center of Gravity." This is not a term used in common parlance, but indicates a certain familiarity with military concepts. One security analyst reports Al Qaeda makes "strategic decisions with detached, methodical precision, constantly assessing alternative approaches as well as seeking additional means or methods."[73] Al Qaeda's familiarity with military concepts combined with a tendency to adapt organizational behavior means that anticipating a more robust understanding of COG analysis by Al Qaeda can prevent a strategic shock. In fact, the incorporation of systems analysis and COG determination is explicitly and widely available in the Joint Publication 5.0, via the internet.[74] Such a methodology of anticipating target selection by past behavior and communicated intent is in keeping with research conducted by the U.S. Secret Service. Consequently, it is not necessarily a stretch to think Al Qaeda strategy may evolve as they attempt to accomplish what they propose publicly and vociferously.

Extrapolation from the September 11, 2001 Attack

The attack of September 11, 2001 was reported to have resulted in the loss of over one million jobs and caused a drop of three percent in U.S. Gross Domestic Product (GDP).[75] A Congressional Research Service (CRS) report claimed the direct effect of the September 11, 2001 attack was not significant enough to cause a long-term economic impact to the nation as a whole.[76] Although the specific macroeconomic impact is not concretely identifiable due to the economy previously beginning to show signs of slipping into a recession, it is difficult to deny the attacks had a large, negative effect on various economic sectors such as the aviation industry and the local economy, particularly the city of New York. Even though the CRS report dismissed the long-term macroeconomic effect of the September 11, 2001 attack, many economists believe the attack had a detectable, negative impact on the U.S. economy at the macroeconomic level in the short term.[77]

Nonetheless, the CRS provides a "blue print" for what an attacker needs to do to have a significant macroeconomic impact. Specifically, the CRS states an attack would have to cause major indirect effects, principally in the areas of consumer confidence, a form of financial panic that leads to decreased foreign investment and increased spending on security, as well as introduce a price shock via energy costs.[78] The CRS report also noted that in times of international crisis, investors typically seek safety for their assets in the United States. However, in the instance of the September 11, 2001 attack, the international crisis was occurring in the United States. Consequently, there was a "short run decline in the net purchases of U.S. assets by foreigners."[79] Although there was no panic selling and no run on the dollar after the aftermath of the September 11, 2001 attack, all trading of U.S. Treasury securities was stopped for two days, and

the stock market was closed for six days.[80] As witnessed during the recent mortgage and banking crisis leading to the current U.S. recession, the role of the Federal Reserve in preventing a complete financial collapse was instrumental. The same was true after the September 11, 2001 attack, when the Federal Reserve issued the following statement: "the Federal Reserve System is open and operating. The discount window is available to meet liquidity needs."[81] The CRS report credits this action by the Federal Reserve with prevention of a potential financial panic. However, this particular vulnerability from the September 11, 2001 attack can be expanded and exploited using a parallel attack on the U.S. economic system.

Some might argue Al Qaeda was only able to coordinate the September 11, 2001 attack as the result of luck. Perhaps luck was involved, but regardless, if Al Qaeda is indeed seeking to attack the U.S. center of gravity (economic power) as it claims, then a feasible strategy can be devised by extrapolating from existing information to achieve a devastating, direct effect on the U.S. economy. As the CRS report indicated, a parallel attack to achieve a desired negative macroeconomic effect would need to achieve a loss in consumer confidence, a financial panic that leads to decreased foreign investment, and a price shock by way of increased energy costs. Adapting Warden's Five Ring Model previously discussed and the concept of parallel attacks, Al Qaeda would need to attack economic leadership, economic organic essentials, key economic infrastructure, the population and defensive system.

Specifically, Warden's Five Ring Model can be adapted to show a crude methodology that could be used by an attacker, based upon the requirements outlined by the CRS report to inflict damage on the U.S. economic system.

Warden's Five-Ring Model	Adapted Construct
Leadership	Assassination of the Federal Reserve Chairman and the Treasury Secretary
Organic Essentials	Cyber-attack(s) on the U.S. financial system and New York City (Manhattan).
Infrastructure	Exploding a WMD (Dirty Bomb) at major shipping port, U.S. oil refineries or electrical grid.
Population	Random attack(s) on airport terminal or subway.
State / Local Security Network	Attack(s) on first responders.

Table 1.

Although this type of attack involves more complex planning, the attacks do not need to be a precision operation occurring at the same time, but can be near-simultaneous to have the desired effect. Various attack methods could be combined that have already been used or have been planned for use by Al Qaeda. For instance, Al Qaeda has previously attempted to use political assassination, hybrid vehicle-bombs, shoulder fired anti-aircraft missiles and planned to acquire and use WMD.[82] These foiled terrorist attacks illustrate a propensity by Al Qaeda to attack significant targets that individually, could have a large economic effect. If the individual attacks were conducted in parallel specifically intended to disrupt the economic system of the U.S., the indirect effects could be catastrophic.

In this hypothetical scenario, the first and most difficult task involves an attack designed to affect the leadership of the U.S. economic system. In this case, it would involve the assassination of the Federal Reserve Chairman who is appointed to his position by the President of the United States and confirmed by the Senate. Replacing the Federal Reserve Chairman could be done in an expeditious manner following an emergency. Unfortunately, the new Chairman certainly would not inspire the same level of confidence to foreign investors when assuring the market of an ability to meet liquidity needs following a successful assassination. This particular scenario is not far removed from the reported planned attempts of Khalid Sheikh Mohammed to assassinate Pope John Paul II and former President Bill Clinton.[83]

Second, a cyber-attack on the U.S. financial banking system would affect the organic essentials or second ring of the U.S. economic system. The U.S. Secret Service in a study of potential cyber threats determined "most incidents required little technical sophistication" and were conducted easily by inside employees.[84] Such a direct attack to the financial system or even an indirect attack similar in scope to a Wiki-Leaks disclosure may compromise consumer confidence to such an extent the entire financial system might be paralyzed.

A third attack to the third ring or economic infrastructure could be utilized to further erode consumer confidence by negating the use of a U.S. major shipping port or power generation plant. A 2002 West Coast longshoreman strike was estimated to potentially cause $19.4 billion in economic losses during a 10 day shutdown and $48 billion for a 20 day shutdown of the affected ports.[85] Aside from the direct economic impact, the potential indirect effect to the economic system as a whole must also be

considered. A dirty bomb might contaminate a port access chokepoint preventing workers access for a significant period of time or affect the cargo cranes thereby severely limiting trade. This type of attack with a dirty bomb was the same method attributed to Jose Padilla during his arrest in 2002 as well as the disrupted plan involving Dhiren Baroot in 2004 against a target in the United Kingdom.[86] Additionally, an attack on an oil refinery such as the foiled plot involving Michael Reynolds who planned to destroy gas pipelines and energy infrastructure in 2005 would drive up the price of gasoline and oil. An increase in gasoline and oil prices would qualify as an energy price shock that would ripple through the economy increasing costs to businesses dependent upon any form of transportation. The CRS analyzed the economic impact on the Gulf region following Hurricane Katrina and noted there is a correlation between most recessions and higher oil prices.[87]

As for attacks on the fourth ring, the U.S. population, random attacks in malls, subways, etc., would be detrimental to consumer confidence, but perhaps not as much as an attack at a major airport terminal. Since most of the Transportation Security Administration (TSA) security and screening is geared for protecting the airplanes from being hijacked or destroyed in flight, a significant economic effect could be achieved by attacking a busy airport terminal where the ticket counters are located. An attack on a large airport terminal such as Atlanta Hartsfield or Chicago O'Hare would have an enormous impact on the entire air travel system. The airport might not be destroyed but the airport and others around the nation would be severely disrupted and possibly, temporarily shut down.

The fifth ring involves attacking the U.S. defensive system. In this example, attacks on the first responders would slow down recovery efforts, affecting governmental response to any crisis. An attack on first responders following an initial attack would add confusion to recovery efforts, exacerbate the effects of the initial attack and cause untold indirect effects.

In outlining such a hypothetical scenario, the main point is to highlight the severe impact of parallel attacks combined with a systems-designed targeting approach. This hypothetical scenario is not provided to determine the most probable method of attack or to provide a commentary on the probable next target. One should not however, given the history of Al Qaeda's tendency to adapt organizational behavior, be surprised if parallel attacks are used in the future and combined with a systems approach for targeting U.S. centers of gravity. In this hypothetical scenario, each of the individual targets selected using the Five Ring Model is based on a published, foiled Al Qaeda attack. Additionally, given Al Qaeda's use and understanding of military concepts, one can anticipate more sophisticated enemy thinking in the future.

Conclusion

By incorporating a systems approach and the concept of parallel attack to existing methodology, the DHS strategy can fully leverage their stated risk components of consequence, vulnerability and threat (R = f(C,V,T)).[88] Although Warden's Five Ring Model was utilized in the Desert Storm air campaign, it certainly can be adapted for use in homeland security planning. By doing so, security planners can better understand the potential consequence of multiple, critical infrastructure or key resources being destroyed or neutralized for a short period of time particularly with respect to the economy as a whole. The Five Ring Model also provides planners with a methodology

for greater understanding of system vulnerability and how parallel attacks might affect larger economic systems or even the entire national economic system, transcending individual sectors. Finally, security planners can better assess targeting probabilities should Al Qaeda attack the U.S. center of gravity espoused by Al Qaeda leaders, the U.S. economy. Al Qaeda has shown a keen ability to adapt and evolve, and the security community in the United States must be able to do the same. The combination of systems thinking and parallel war can help planners more effectively secure the homeland against future attacks.

Endnotes

[1] Jena Baker McNeil, James Jay Carafano, and Jessica Zuckerman, *30 Terrorist Plots Foiled: How the System Worked,* Background Paper (Washington D.C.: The Heritage Foundation, 2010),1, http://thf_media.s3.amazonaws.com/2010/pdf/bg_2405.pdf (accessed November 6, 2010).

[2] Barry Meier and Eric Lipton, "In Air Cargo Business, It's Speed vs. Screening, Creating a Weak Link in Security," *New York Times*, November 2, 2010.

[3] Germain Difo, *Ordinary Measures, Extrordinary Results: An Assessment of Foiled Plots Since 9/11,* Security Policy Paper (Washington D.C.: American Security Project, 2010),12-25, http://americansecurityproject.org/wp-content/uploads/2010/09/Foiled-Plots.pdf (accessed November 6, 2010).

[4] John A. Warden, III, "The Enemy as a System," *Airpower Journal*, 515, no. 1, (Spring 1995) http://www.airpower.maxwell.af.mil/airchronicles/apj/apj95/spr95_files/warden.htm (accessed November 6, 2010).

[5] Difo, *Ordinary Measures,* 1.

[6] Dennis C. Blair, *Annual Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence,* (Washington D.C.: Office of the Director of National Intelligence, February 2, 2010), 8, http://intelligence.senate.gov/090212/blair.pdf (accessed November 6, 2010).

[7] Brian M. Drinkwine, *The Serpent In Our Garden: Al-Qa'ida and the Long War,* Strategic Research Project (Carlisle Barracks, PA: U.S. Army War College, January 2009), 1.

[8] Warren S. Eller and Brian J. Gerber, "Contemplating the Role of Precision and Range in Homeland Security Policy Analysis: A Response to Mueller," *Policy Studies Journal*, 38, no. 1, (February, 2010), 33; Department of Homeland Security, *Right Wing Extremism: Current*

Economic and Political Climate Fueling Resurgence in Radicalization and Recruitment, (Washington D.C.: Department of Homeland Security, 2009), 7-8, http://www.fas.org/irp/eprint/rightwing.pdf (accessed January 8, 2011).

[9] Difo, *Ordinary Measures,* 27.

[10] Brian Michael Jenkins, *Basic Principles for Homeland Security,* testimony before the House Appropriation Committee, Santa Monica: RAND Corporation, (2007), 2, http://www.rand.org/pubs/testimonies/2007/RAND_CT270.pdf (accessed November 6, 2010).

[11] Brain A. Jackson and David R. Frelinger, *Emerging Threats and Security Planning,* Occasional Paper (Santa Monica: RAND Corporation, 2009), 1, http://www.rand.org/pubs/occasional_papers/2009/RAND_OP256.pdf (accessed November 6, 2010).

[12] Joint Chiefs of Staff, *Joint Operations Planning, JP 5.0* (Washington D.C.: Department of Defense, 2010), III-21.

[13] Ibid., III-21.

[14] Ibid.

[15] Ibid., III-22.

[16] Rudolph M. Janiczek, "A Concept at the Crossroads: Rethinking the Center of Gravity," Strategic Research Paper (Carlisle Baracks, PA: U.S. Army War College, 2007), 5-10, http://www.strategicstudiesinstitute.army.mil/pdffiles/pub805.pdf (accessed November 6, 2010).

[17] Antulio J. Echevarria II, *Clausewitz's Center of Gravity: Changing Our Warfighting Doctrine-Again!,* (Carlisle Barracks, PA: U.S. Army War College, 2002), 10, http://www.strategicstudiesinstitute.army.mil/pubs/download.cfm?q=363 (accessed November 6, 2010).

[18] Ibid., vii.

[19] Warden, "The Enemy as a System," 2.

[20] John A. Warden, III, "Air Theory for the Twenty-first Century," in *Battlefield of the Future,* ed. Barry R. Schneider and Lawrence E. Grinter (Maxwell AFB, AL: Air University Press,1995). http://www.airpower.maxwell.af.mil/airchronicles/battle/chp4.html (accessed October 17, 2010), 6.

[21] Ibid.

[22] Ibid., 4.

[23] Ibid., 8.

[24] Ibid., 7.

[25] Ibid.

[26] Ibid., 9.

[27] David A. Deptula, *Effects-Based Operations: Change in the Nature of Warfare,* (Arlington: Aerospace Education Foundation, 2001), 1-6, http://www.aef.org/ pub/psbook.pdf (accessed October 17, 2010).

[28] Warden, "The Enemy as a System," 12.

[29] Ibid., 7.

[30] Deptula, *Effects-Based Operations*, 6.

[31] Ibid., 6.

[32] Ibid., 5.

[33] Ibid., 25.

[34] Henry H. Willis, *Risk Informed Resource Allocation at the Department of Homeland Security,* (Santa Monica: RAND Corporation, 2007), 2, http://www.rand.org/content/dam/rand/pubs/testimonies/2007/RAND_CT272.pdf (accessed October 17, 2010).

[35] Ibid., 2.

[36] Jackson and Frelinger, *Emerging Threats and Security Planning,* 10.

[37] Willis, *Risk Informed Resource Allocation at the Department of Homeland Security*, 1.

[38] Ibid., 3.

[39] John Mueller, "Assessing Measures Designed to Protect the Homeland," *Policy Studies Journal*, 38, no. 1 (February, 2010), 2, http://psweb.sbs.ohio-state.edu/faculty/jmueller/isa9psjx.pdf (accessed November 6, 2010).

[40] Ibid., 11.

[41] Ibid.

[42] George W. Bush, *Homeland Security Presidential Directive, HSPD-7*, (Washington D.C.: U.S. Government, 2003), http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm#1 (accessed January 8, 2011).

[43] Department of Homeland Security, *The Physical Protection of Critical Infrastructures and Key Assets,* (Washington D.C.: Department of Homeland Security, February, 2003), 2, http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf (accessed October 17, 2010).

[44] John D. Moteff, *Critical Infrastructures: Background, Policy, and Implementation,* Report for Congress (Washington D.C.: Congressional Research Service, 2010), 10, http://www.fas.org/sgp/crs/homesec/RL30153.pdf (accessed October 17, 2010).

[45] Ibid., 27.

[46] Eller and Gerber, "Contemplating the Role of Precision," 42.

[47] Mueller, "Assessing Measures Designed to Protect the Homeland," 4.

[48] Ibid., 1.

[49] Ibid., 3.

[50] Eller and Gerber, "Contemplating the Role of Precision," 43.

[51] Ibid.

[52] Department of Homeland Security, *National Infrastructure Protection Plan,* (Washington D.C.: Department of Homeland Security, 2009), 1, http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf (accessed November 6, 2010).

[53] Ibid., 27-48.

[54] Ibid., 28.

[55] Ibid.

[56] Ibid., 32.

[57] Ibid., 34.

[58] Department of Homeland Security, *National Planning Scenarios: Executive Summaries*, (Washington D.C.: Department of Homeland Security, July, 2004), http://www.scd.hawaii.gov/grant_docs/National_Planning_Scenarios_ExecSummaries_ver2.pdf (accessed November 6, 2010).

[59] Department of Homeland Security, *National Infrastructure Protection Plan*, 35.

[60] Ibid.

[61] Moteff, *Critical Infrastructures: Background, Policy, and Implementation,* 26.

[62] Department of Homeland Security, *The Physical Protection of Critical Infrastructures and Key Assets,* 7.

[63] Eller and Gerber, "Contemplating the Role of Precision," 32.

[64] Ibid., 33.

[65] Counterterrorism Coordinator Richard Clarke, "Strategy for Eliminating the Threat from Jihadist Networks of Al Qida: Status and Prospects," memorandum for National Security Advisor Condoleeza Rice, Washington D.C., declassified December 2000, http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB147/clarke%20attachment.pdf (accessed October 12, 2010).

[66] Randy Borum et al., "Threat Assessment: Defining an Approach for Evaluating Risk of Targeted Violence," *Behavioral Sciences and the Law*, 17, no. 3, (1999), 329, http://www.secretservice.gov/ntac/ntac_bsl99.pdf (accessed October 17, 2010).

[67] Ibid., 330.

[68] McNeil, Carafano, and Zuckerman, *30 Terrorist Plots Foiled,* 1-16.

[69] Borum et al., "Threat Assessment," 332.

[70] Jenkins, *Basic Principles for Homeland Security,* 3.

[71] Drinkwine, *The Serpent In Our Garden,* 17-19.

[72] Sarah E. Zabel, *The Military Strategy of Global Jihad,* Strategic Research Paper (Carlisle Barracks, PA: U.S. Army War College, Strategic Studies Institute, 2007), 6, http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB809.pdf (accessed October 17, 2010).

[73] Drinkwine, *The Serpent In Our Garden,* 17.

[74] This information regarding systems analysis and center of gravity determination is available via the Joint Publication 5.0 and can be found at this website: http://www.dtic.mil/doctrine/new_pubs/jp5_0.pdf (Accessed 15 Jan 2011).

[75] Nick Bloom, *The Economic Impact of 9/11,* Policy Brief (Stanford: Stanford Institute for Economic Policy Research, 2007), 1, http://www.stanford.edu/~nbloom/uncertaintyshocks_SIEPR.pdf (accessed November 6, 2010).

[76] Gail Makinen, *The Economic Effects of 9/11: A Retrospective Assessment,* (Washington D.C.: Congressional Research Service, 2002), CRS-9, http://www.fas.org/irp/crs/RL31617.pdf (accessed November 6, 2010).

[77] Bryan W. Roberts, *The Macroeconomic Impacts of the 9/11 Attack: Evidence from Real-Time Forecasting,* Policy Paper (Washington D.C.: Department of Homeland Security, Office of Immigration Statistics, August, 2009), 4, http://www.dhs.gov/xlibrary/assets/statistics/publications/ois_wp_impacts_911.pdf (accessed November 6, 2010).

[78] Gail Makinen, *The Economic Effects of 9/11,* CRS 3-12.

[79] Ibid., CRS-3.

[80] Ibid., CRS-10.

[81] Ibid.

[82] Difo, *Ordinary Measures,* 23.

[83] McNeil, Carafano, and Zuckerman, *30 Terrorist Plots Foiled:,* 11.

[84] Marisa Reddy Randazzo, Michelle Keeney, and Dawn Cappelli, *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector,* Assessment (Washington D.C.: U.S. Secret Service and CERT Coordination Center, 2004), 7, http://hornbeam.cs.ucl.ac.uk/hcs/teaching/GA10/lec4extra/certreport.pdf (accessed October 17, 2010).

[85] Paul Nyhan, "Longshoremen strike or lockout could stagger nation's economy." *SEATTLE POST-INTELLIGENCER .* June 10, 2002, http://www.seattlepi.com/business/73906_longshore10.shtml (accessed October 31, 2010).

[86] Difo, *Ordinary Measures, Extrordinary Results,* 12*,* 16.

[87] Brian,Cashell and Marc Labonte, *The Macroeconomic Effects of Hurricane Katrina,* (Washington D.C.: Congressional Research Service, 2005), 4, http://fpc.state.gov/documents/organization/53572.pdf (accessed January 8, 2011).

[88] Department of Homeland Security, *National Infrastructure Protection Plan*, 32.