TINMORE INSTITUTE
Tomorrow's solutions today!

CENTER FOR ENERGY SECURITY
CENTER FOR WATER SECURITY
CREATIVE INTELLIGENCE
ECONOMICS & FINANCE
GLOBAL RESOURCES SECURITY
KNOWLEDGE MANAGEMENT
MAPPING HUMAN BEHAVIOR
SCIENCE & TECHNOLOGY

December 2014

About Research Reports
E-Distribution Rights
Feedback Welcome

Support TINMORE INSTITUTE
Browse Reports & Bookstore
Make a donation

Contact Us
www.tinmore.com

Secure Technology, Centers of Gravity and Homeland Security

Robert Boyd

TinMore Institute Research Report HS140115

Disclaimer

The opinions and comments contained herein are solely those of the author(s) and do not represent the views, policy, or opinions of any local, state or national government, private corporation(s), or other corporate, institutional, or academic entities of any kind. Mention of a specific tool, software, or product does not affirm endorsement of the item(s) nor of the entity that markets and/or manufactures said item(s). Finally, reference of a specific corporation, firm, or government agency does not constitute author(s) endorsement of them or endorsement by the agency(s) or firm(s) for which the author(s) work.

Secure Technology, Centers of Gravity and Homeland Security

Robert Boyd

TIRRHS140115

Executive Summary

Critical Infrastructure Protection was a growing national security concern prior to the terrorist attack of September 11, 2001. “The United States possesses both the world’s most advanced military and its largest economy. These two aspects of power are mutually reinforcing and dependent”.[1] The security scales inside this document highlight layers of protection using the capacities of the federal, state, and local governments, to incorporate Public-Private Partnership to Reduce Vulnerability. Nonetheless, as an outcome of advancements and evolution in information technology and the commitment of improved efficiency, many layers of security have become increasingly automated and interlinked. Identifying United States Centers of Gravity (COGs) and adopting a comprehensive systems assessment a useful framework can be added to the living homeland security toolkit to reinforce domestic security.

This paper discusses the traditional COG concept, leverages deductive reasoning to examine operational security, and explores information assurance issues comparative to technology and critical infrastructure to evaluate what these issues mean to potential adversaries and the U.S. government. John Warden’s Five Ring Model is utilized as a framework for analysis to develop a viable comprehensible picture of “complex phenomenon so that we can do something with it”.[2] Finally, a conjectural set of scenarios are introduced to illustrate the usefulness of systems thinking to homeland security.

[1] The White House, *Critical Infrastructure Protection. Presidential Decision Directive/NSC-63, 1998* (Washington, DC: 1998).

[2] James .A. Warden’s III, “The Enemy As A System” *Air Power Journal*, Spring 1995.

INTRODUCTION

Today's interconnection of cyberspace technologies and physical domains has resulted in increased efficiency in telecommunications, energy, banking and finance, water systems and emergency services, both government and private. Enabling multiple points-of-access to facilitate remote operations has optimized the management of these critical infrastructures. As a result of this convergence, however, these multiple points-of-access have also resulted in increased vulnerability and exposure to disruption. The intricacy of technology has left systems exposed to non-traditional strikes on infrastructure and information systems. "Perhaps the most well known event is the Chernobyl nuclear reactor disaster, April 1986 in Ukraine, which resulted from a low-power systems test and subsequent severe release of radioactivity following a massive power excursion that destroyed the reactor." [3] Although a shortened depiction of the above event, continued dependency on technology systems with ill-defined security could lead to greater threats.

Analyses of enemy foiled plots reveal a wide array of targets to include bridges, major financial institutions, the New York Stock Exchange and various critical infrastructure assets".[4] Coupled with cyber attacks on Press TV, NASA, the State Department, Commerce Department, the Naval War College, and others systems, highlights an alarming concern to homeland security and heightened call for protection of critical infrastructure-government and state. In response, the U.S. government in an effort to provide security systems aimed at providing multiple layers of protection, launched a program to thwart cyber attacks on critical infrastructure at the federal, state, and local government level.

> *The administration has quietly launched Perfect Citizen, a digital surveillance project to be run by the NSA; the project's goal is to detect and detect cyber attacks on private companies and government agencies running critical infrastructure such as the electricity grid, nuclear-power plants, dams, and more; the program would rely on a set of sensors deployed in computer networks for critical infrastructure that would be triggered by unusual activity suggesting an impending cyber attack — although it would not persistently monitor the whole system* (Homeland Security Wire, 2010)

Although some security experts see this as triumph in quickly establishing a robust program, additional efforts remain necessary. "Operational systems are increasingly subject to cyber attacks, as many are built around legacy technologies with weaker protocols that are inherently more vulnerable".[5] To date, the Department of Homeland Security (DHS) recognizes a prime sector, energy (electricity, petroleum, and natural gas) as part of critical infrastructure assets. "So vital to the United States that its incapacitation or destruction would have debilitating effects on security, national economic security, public health or safety, or any combination thereof".[6] However, DHS has yet to mandate 'cyber controls' over a myriad of these holdings.

[3] James A. Tindall and Andrew A. Campbell, *Water Security: Conflicts, Threats and Policies* (Colorado: DTP Publishing, 2012), 22.

[4] Germain Difo, *Ordinary Measures, Extraordinary Results: An Assessment of Foiled Plots Since 9/11* (Washington D.C. American Security Project, 2012) 12-25

[5] PricewaterhouseCoopers, *Cyber Attacks: Is Your Critical Infrastructure Safe*, www.pwc.com/us/en/industry/utilities/assets/cyber-attacks.pdf *(accessed 28 Aug. 2012)*

[6] Ibid, 4.

By identifying and analyzing centers of gravity and embodying across-the-board systems assessment, a functional framework can potentially strengthen linkages between virtual and infrastructure defenses. Its purpose, to identify crucial targets and conduct analysis of the risk posed by potential adversaries attempting to unsettle or destroy critical infrastructure leveraging technology systems and poor information assurance. To that end, Center of Gravity and Systems analysis serve as platforms to assist in illustrating multiple aspects and vulnerabilities as a result of interconnectedness of critical infrastructure and cyber.

CENTER OF GRAVITY AND SYSTEMS ANALYSIS

Developing a comprehensive homeland security and defense strategy to defend the United States is an inherently dynamic and complex task. The complexity of strategy development that accounts for the numerous variables and factors that define critical infrastructures requires that this problem set be examined as a whole and not as a small fragment. Joint doctrine and military theory mandates the appraisal of an adversary using a Center of Gravity (COG) approach to assist in determining strengths, weaknesses, and gaps. Defined, it is "a source of power that provides moral or physical strength, freedom of action or will to act. COG is what the Prussian theorist Carl von Clausewitz called "the hub of all power and movement, on which everything depends".[7]

In assessing the adversary's COG, it is prudent to employ this approach to perceive and review both the "forest and the trees"[8] instead of the sum of the individual components. It is the process of identifying COGs that function as a basis for identifying sources of power as well as sources of critical vulnerability. [9] Adapting such a bifocal vantage point for homeland security, particularly towards critical infrastructure vulnerabilities and cyberspace, provides security planners and policy makers with an analytical blueprint to understand the nation's power centers (human dimensions to the technical, static to dynamic, cognitive, inputs and outputs, etc.) and assign defensive positions correspondently.

The United States as a whole is a complex body in terms of governance, economic systems, military forces and national infrastructure; one has a very difficult time attempting to identify one decisive point.[10] Hence, examining interrelationships rather than pursuing linear cause-effect chains is an integral and mandatory part[11] of COGs and systems analysis. It, undoubtedly, is why a COG framework is practical but can be complex to embody the full range of foreseeable inclusions internal and external to the system. In short, this approach is both adaptable and flexible. As a result, Clausewitz's theory of COG when appropriately applied using the enemy as a whole, or system, is still valid and applicable. To this point, understanding the facets that influence the integrity of security-as the nexus to cyber and critical infrastructure as whole- is the key to making a COGs and System analysis concept useful.

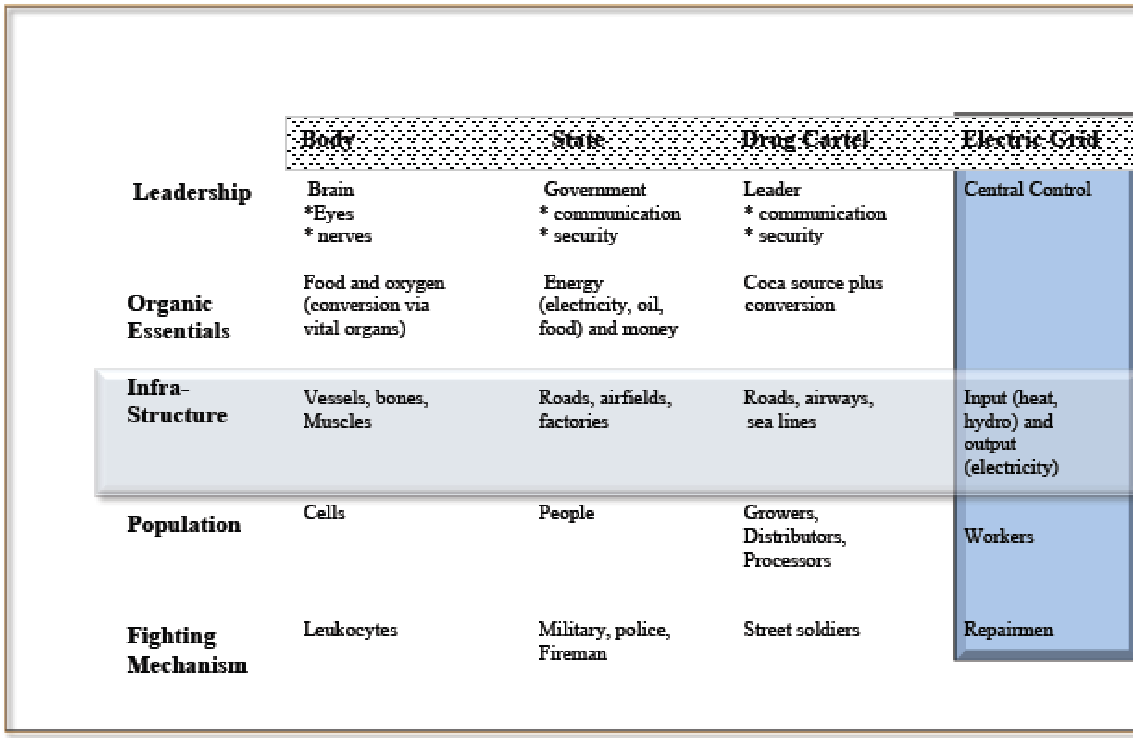
[7] Echevarria II, A.J. (2002). Clausewitz's Center of Gravity: Changing Our Warfighting Doctrine-Again? http://www.carlisle.army.mil/usassi/welcome.htm (accessed 28 Aug. 2012).
[8] Edson, R. (2008) Systems Thinking Applied. PRIMER v1.1, 5.
[9] Joint Chiefs of Staff, *Joint Operations Planning*, JP 5.0 (Washington D.C.: Department of Defense, 2010) III-21.
[10] Rodriguez, D. US Army War College "Systems Analysis, Centers of Gravity and Homeland Security". www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA553442 *(accessed 28 Aug. 2012).*
[11] Edson, R. (2008) Systems Thinking Applied. PRIMER v1.1., 14.

One central mechanism for use in better understanding how COGs and systems thinking is applied is through utilization of Colonel John Warden's perception of viewing the "enemy as a system" and associated Five Ring Model as a applicable tool to accompany Wardens assertion:

> *There are basically two ways to think: inductively and deductively. The first requires gathering many small facts to see if anything can be made of them. The second starts with general principles from which details can be learned. The first is tactical and the second is strategic… to become good operational artists and strategists, however, we must learn to think deductively.* (The Enemy as a System, 1995)

Although Warden's Five Ring Model may hold surveying examinations by some as a result of the environment in which the model was applied, it proves applicable proportional to understanding how targets may be attacked. Warden's Five Ring Model is based upon the proposition that all human organizations, including societies, are designed similarly and share certain characteristics.[12] As depicted in Warden's model in Figure 1, underneath infrastructure, the enemy can leverage gaps in security to gather and disseminate information to enemy forces. These gaps in security, and connections to computer-controlled systems may potentially hold critical infrastructure at risk.

Table 1. Modified John A. Warden III table examining five rings with a human-body approach



	Body	State	Drug Cartel	Electric Grid
Leadership	Brain *Eyes * nerves	Government * communication * security	Leader * communication * security	Central Control
Organic Essentials	Food and oxygen (conversion via vital organs)	Energy (electricity, oil, food) and money	Coca source plus conversion	
Infra-Structure	Vessels, bones, Muscles	Roads, airfields, factories	Roads, airways, sea lines	Input (heat, hydro) and output (electricity)
Population	Cells	People	Growers, Distributors, Processors	Workers
Fighting Mechanism	Leukocytes	Military, police, Fireman	Street soldiers	Repairmen

[12] Barry R. Scheneider and Lawrence E. Grinter and John A. Warden, III A*ir Theory for the Twenty-first Century* (University Press of the Pacific (April 1, 2002), Ch. 4

Systems require a form of organic essentials; some form of input energy, and the prerequisites to convert it to another form...Without these, the brain cannot perform its strategic function, without the brain, these organs don't get the commands they need to provide integrate support. [13] Understanding this logic, assist in pinpointing the personal strategic center- the brain. Without understanding what to protect relative to security, critical infrastructure is exposed to threats from most anywhere. With critical infrastructure being at risk to threat, further discernment of the gaps in security to mitigate the threat become paramount.

There are those who believe a depiction of green lights across display boards and monitors assert that systems put in place to monitor 'x and y' are functioning the way they have been programmed. This is errant, unfortunately, "no machine can take over strategic functions from the brain".[14] Thus, a better identification of the threat, especially as it relates to cyberspace and critical infrastructure, will only serve to strengthen security planners' ability to identify and mitigate such security vulnerabilities.

The extreme interconnectedness of the U.S. Economic system could make the U.S. vulnerable to an attacker who could exploit security through use of concepts of parallel war across multiple domains. Identification of the enemy's real target and better coordination of military, law enforcement, political and economic actors to develop a comprehensive and integrated defense strategy is paramount; specifically, as it relates to cyber-security and critical infrastructure.

A PERSISTENT THREAT

Cyberspace Presence

The *Wall Street Journal* published online late Thursday (July 21, 2012) on the new cybersecurity bill…called the Cyber security Act of 2012. The bill would provide legal immunity and a structured system for private companies and U.S. intelligence agencies to share information about national cyber threats".[15] Although security measures are being implemented by the United States Government (USG); it is not altogether clear that the existing methodology adopted would protect the U.S. from more catastrophic events demonstrated as potential risk by the president and top defense and intelligence officials.

In the past, conventional attacks primarily used widespread broadcast aimed at computer systems deployed on networks. Now, malign activity has become more web-based as assailants are targeting end-users instead of computers. More so, a robust underground economy consolidating and maturing with capability and duty to adapt rapidly, to the end certain regions are being affected globally. In 2007, Symantec observed 87,963 intrusion attempts, an increase of 167 percent. "Globally, 66 percent of all intrusion Web sites identified by Symantec were located in the United States. "The majority of brans used in attacks were in the financial service".[16]

Former Department of Homeland Security (DHS) Secretary Janet Napolitano publicly validated her belief in an increasing threat saying " Hackers have " come to close" several times to shutting down

[13] Barry R. Scheneider and Lawrence E. Grinter and John A. Warden, III A*ir Theory for the Twenty-first Century* (University Press of the Pacific (April 1, 2002), Ch. 4

[14] John A. Warden III "The Enemy As A System," *Airpower Journal*, Spring 1995

[15] TPMIdeaLab, *Cybersecurity Bill Backed By Obama Won't Protect U.S., Experts Agree*, 07 July 2012 (accessed 04 Sept. 2012).

[16] Symantec. Internet Security Threat report, Volume XIII, April 2008.

elements of the nation's infrastructure…Wall Street firms and transportation systems are frequent cyber attack targets".[17] The need for an "army of cyber geeks" may be drastically overplayed along with the notion of the next 'cyber pearl-harbor'. Nevertheless, external and internal vulnerabilities of the interconnectedness and loose management and security protocols relative to cyber pose a serious challenge to DHS security planners and other stakeholders.

> *Telecommunications was the top critical infrastructure sector for malicious activity in the last half of 2007, accounting for 95 percent of the total. The top country of origin for attacks targeting the government sector was the United States, which accounted for 21 percent of the total. This is an increase from the first half of 2007 when the United States accounted for 19 percent of the total. Denial-of-service attacks were the most common attack type targeting government and critical infrastructure organizations, accounting for 46 percent of the top ten attacks. This is a decrease from the first half of 2007, when denial-of-service attacks accounted for 35 percent of the total and ranked second.* (Symantec Internet Security Threat Report, 2008)

Within the context of a tenacious threat from groups whom possess the capability and willingness to leverage poor security practices between physical critical infrastructure and virtual built frameworks, caution commands security planners conduct a comprehensive review of existing security measures. Observations by Germain Difo, an analyst for the American Security Project, disputes now is the time to resolve which methods have been effective, which methods are too costly, and the best way to conform and prepare for the future.[18] As an example, "The vulnerability and centrality of computer systems in the U.S. water infrastructure raises the threat of embedded terrorists or moles in key water infrastructure…"(Tindall and Campbell, 2012). [19] As technological platforms connect with physical stations, the level of awareness and security vulnerability increases.

A prime example of this unknown security vulnerability has been found in terrorist groups as the Mujahid. Their practice of a fresh form of terrorist counterintelligence poses an unused framework of assessing the threat for homeland security planners. Given the interconnection and complexity of the political, economic, energy, environmental and social systems in the United States, the prospective targets are virtually endless to groups where their focus is antagonistic of what security analyst decrees needs safeguarding. The overwhelming concern for the protection of critical infrastructure is key, but believe the room for exploitation of it through auxiliary means of interconnection (further outside the system) is just as important.

The technological Jihad, as Tindall describes it, is "a main pillar in the battle of Islam against the Crusaders and the polytheist belief".[20] The Jihad, in its second issue published in Arabic, a periodical organized in varying sections, on technical training. These sets of training spread across some of the more demanding platforms from network encryption, Morse code to binary symmetrical encryption keys; by far, some of the more demanding encryption algorithms used in cryptography software today.

[17] Ed O'Keefe "Hackers have "come close" to major cyberattack" *Washington Post*, 27 Oct. 2011 (accessed 04 Sept. 2012).

[18] Germain Difo, *Ordinary Measures, Extraordinary Results: An Assessment of Foiled Plots since 9/11* Security Policy Paper (Washington D.C.: American Security Project, 2010), 12-25

[19] James A. Tindall and Andrew A. Campbell, Water Security: Conflicts, Threats and Policies (Colorado: DTP Publishing, 2012), 279.

[20] Ibid, 279

One of the more powerful forms of non-kinetic threats to security (that uses a network platform) is psychological warfare. Psychological terrorism through use of online forums is possibly one of the easiest methods to convince followers to do most anything.

Journey back to 2002, when Imam Samudra was convicted of masterminding the bombing that killed 202 in Bali, Indonesia. In his manifesto, he wrote that he rose funding for terrorism through use of cyber fraud. One chapter in his proclaimed autobiography titled “Hacking, Why Not”? “Directs fellow Muslim radicals to Web sites and chat rooms for instructions on online credit card fraud and money laundering”.[21] Samudra writes "Any man-made product contains weakness because man himself is a weak creature," So it is with the Americans, who boast they are a strong nation".[22] This surge in activity has given counterterrorism specialist, already concern with threats to physical structures, another worry. Given this dynamic, the overwhelming consideration for the U.S. government interagency framework results in how to strengthen Information Technology and systems while matching wits with a persistent and adaptable adversaries.

> *“As Internet technologies become more advanced, so do those who use them for illicit and illegal activities,” says Dexter Ingram, director of information-security policy for the Business Software Alliance and a former analyst for the House Committee on Homeland Security’s cyber-security subcommittee. “Security must remain a continuous process, It’s a never-ending cycle”.* (USA Today, 2005)[23]

It is clear, however, although technology was the item to take the world into the 21st Century, it became side swiped by physical impediments and action against physical infrastructure, especially the event of September 9/11. The emphasis was on more security to physical infrastructure and preparation on where the next (if were to arise) attack would happen. However, who would have ever fathomed that this was merely a tactic, a deception if you will, to gain an edge over virtual platforms that have been considered vulnerable to intrusion since the early 90s, cyberspace.

> The chase for technology among these groups to gain the necessary knowledge to defeat cyber systems, such as ICS, may only be surpassed by that of the U.S. Department of Defense. Some security experts have implied that the efficacy of this [information among Islamists and Arabic-speaking hackers could prove significant. These groups are determined, persistent, and relentless in their efforts- they should not be readily dismissed (Water Security, 2012).

This is where the adversary has concentrated its efforts most of the last ten years while the United States devoted much time to securing physical infrastructure to virtual indication and warning systems where the adversary has been exploiting. Now that the dependency by the United States to leverage these platforms for indications and warning are so invaluable, how do one-implement security perimeters to push back an internal threat? Therein lie the potential for counterintelligence and the insider threat considerations.

[21] Jon Swartz “Terrorist use of Internet spread” *USAToday.* 20 February 2011.

[22] Ibid.

[23] James A. Tindall and Andrew A. Campbell, Water Security: Conflicts, Threats and Policies (Colorado: DTP Publishing, 2012).

TERRORISTS AND CRITICAL INFRASTRUCTURE

There must be a comprehension of the linkages relative to terrorism, cyberspace and critical infrastructure in order to understand the growing concern of critical infrastructure and vulnerability through interconnectedness. To that end, what exactly is the counterintelligence threat in cyberspace and is it myth or reality? More specifically, can the notion of such events be linked to what many have perceived as a terrorist type act? According to The European Convention on the Suppression of Terrorism, the intent or purpose of a terrorism offense is described via its convention as:

> *By their nature or context to seriously intimidate a population or unduly compel government or an international organization to perform or abstain from performing any act or seriously destabilize or destroy the fundamental political, constitutional, economic or social structures of a country or an international organization.* (Terrorism in Cyberspace-Myth or reality, 2007)

Just as in conventional warfare and security, practices are leveraged to assist in predicting possibilities for terrorism, therein must lay a common understanding of how it applies to security relative to cyberspace and critical infrastructure. The one fundamental baseline is in the motive. “Terrorist acts, whether physical or non-kinetic in mature, “must be designed to spread public fear, and must be made by terrorist intent or motivation”.[24] Intent has been the instrument to comprehend the capacity of terrorist for well over the last decade. What is their political motivation, and how is it tied to the act conducted? However, this logic and is applicability to cyber and critical infrastructure must include a few more variables.

It beckons to contemplate the linkage between terrorism in cyberspace and its association to cyber crime. Even so, intent is not enough to leverage a cyber means to execute an attack on critical infrastructure by terrorist groups or organizations. Security planners must comprehend that systems are full with safeguards, and redundant protocols that prove rather difficult to intrude upon without detection. Thus, in such a case, terrorist organizations or groups must possess not only a measure of intent, but also a capacity to gain access to critical sensitive and compartmentalized information and continual access to the system where it is stored. Schjolberg has made note of a few definitions to better shed light on the linkages. One of which is as follow:

> *Cyberterrorism has been defined as unlawful attacks and threats of attack against computers, networks, and stored information. It has to intimidate or coerce a government or its people in furtherance of political or social objectives. An attack should result in violence against persons or property, or at least cause enough harm to generate fear. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact.* (Terrorism in Cyberspace-Myth of reality, 2007).[25]

Prospective targets may be governmental systems and networks, telecommunications systems, navigation systems for shipping and air traffic, water control systems, energy systems, and financial

[24] Stein Schjolberg, *Terrorism in Cyberspace-Myth or reality?* (2007), 2.

[25] Dorothy E. Denning, Professor USA “Testimony before the Special Oversight Panel on Terrorism” Committee on Armed Services, U.S. House of Representatives, May 2000 (accessed 05 September 12), pg. 2.

systems or other offices of necessary substance to the society. To the point that it begins not to matter if the slowing down being provisional or unchanging or fractional or complete. It is the simple fact that it is happening. The aforementioned, as well as other offensives that have remained concealed from the public can highlight the growing vulnerability exemplified from the interconnectedness of non-kinetic technology and the critical infrastructure platforms being managed, and protected. Who is the threat?

Does the cause for the suspicion lie with the employee (insider) who has access to internal information that is being used to control and manage critical infrastructure platforms? Or is the outsider trying to gain access to networks through exploitation of vulnerabilities seeking to or influence or disrupt the system being used? Regardless, the level of intent, capability, and access by the outsider influencing the insider, or insider with a personal grudge prove why the role of counterintelligence is an essential function to countering a wide spectrum of insider and outsider threats adding to another complex variable within the system.

THE ROLE OF COUNTERINTELLIGENCE

The Outsider

The outsider is often seen as the enemy in the system and can be exploited further as a system itself. "We are at risk. Increasingly, America depends on computers…Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb (Wiemann 2006:2)[26]. The problem that must normally occur relative to the outsider threat (specific to a terrorist act) is how do you define what the terrorist is, and then further defining its association, to be considered a cyber-terrorist?

As the debate ensues as to what constitutes a terrorist attack, the multiplicity of terrorist aims, motives, and ways in which the public views such groups clearly identify the techniques, tactics, and procedures within cyberspace and its ability to conduct violence and spread harm cannot be undermined. The adversary understands how the U.S. conducts intelligence-gathering operations and seeks for ways to deceive us; especially groups such as Al Qaeda. "The five key 9/11 terrorists rejected the U.S. government's accusation of conspiracy. A point from Tindall's water security highlights the mindset and capability of the outsider and its affiliates and organization group's capacity to influence information platforms in an effort to damage critical infrastructure:

> *Were you expected us to inform you about our secret attack plans? Your intelligence apparatus, with all its abilities, human and logistical, had failed to discover our military attack plans before the blessed 11 September operation. They were unable to foil our attack. We ask, why then should you blamed us, holding us accountable and putting us on trail? Blame yourselves and your failed intelligence apparatus and hold them accountable, not us".* (Water Security, 2012)[27]

The infrastructure we leverage to conduct day-to-day business is growing faster than the ability to put methods in place to secure it. The interconnectedness of it all is not thought about by security

[26] Wiemann, G. (2006) 'Cyberterrorism: How Real is the Threat?' United States Institute for Peace, Washington DC

[27] James A. Tindall and Andrew A. Campbell, Water Security: Conflicts, Threats and Policies (Colorado: DTP Publishing, 2012), 279

planners, nor is the mapping and identification procedures to protect it from attacks by foreign and domestic terrorists, especially relative to computer networks and their association with power grids, financial markets and the government. "The history of successful terrorist attacks can be summarized in two words--- "too late".[28] It is imperative to look more closely at the defenses to warn against attack, and shift the focus from developing capacity and capability to launch attacks targeting critical infrastructure through cyberspace.

The Insider

One could hardly comprehend a holistic approach to cyber security and its relationship to critical infrastructure without considering the only danger that ties them both together- the insider threat; a trusted person with access to sensitive systems or information that either deliberately or accidentally compromises them. Most people see the insider threat as a disgruntle employee or someone with access to computer systems above the user level, the IT administrator. However, the reality is that the insider can act in differing ways and various methods to cause harm to the organization.

Cyber attacks are possibly one of the easiest ways for insiders to commit crimes, as the trusted source is the person with continual access and no history to jeopardize security clearance. It is simply illogical to focus efforts solely on cyber security controls. For the most part, the threat resides within the individual, scarcely ever the manner of attack. As Tindall pointed out in *Water Security* the insider can gain almost limitless access as seen by the California Water Service Company employee Addirahman Ismael Abdi in 2005. Abdi worked on a fraudulent H1B visa for the CWSC and eventually resigned his position from the CWSC in April 2009. "On that evening, he used his electronic key card to gain access to the secure electronic gate at the CWSC parking lot then used the computers of two CWSC employees to send over $9 million dollars to three separate accounts in Quatar and fled". [29] As can be seen, this attack was not a demonstration by some adversaries as read seen in previous examples nevertheless, all the more important. Hackers more time than none get away with a bulk of cybercrime. However, the malicious insiders are more likely to get away with it than hackers, and organized crime groups.

Many companies, especially in public organizations, would consider the insider threat to be a high-impact, low frequency type of issue, while the outsider threat is high impact, high frequency. Most no company would relish in it happening on their watch so-to-speak. Thus, implementing management procedures to mitigate if not prevent such an attack is not of high priority. Experts as Tindall assert:

Internal counterintelligence programs are essential to counter a wide spectrum of insider threats ranging from targeted terrorist moles with the target infrastructure to employees, contractors, and sub-contractors who may have direct or indirect affiliations to foreign intelligence services or terrorist patron states, and individuals with untraceable or unverifiable familial tribal ethnic connection to pro-terrorist groups, organizations or regimes (Water Security, 2012).

[28] Ibid, 279

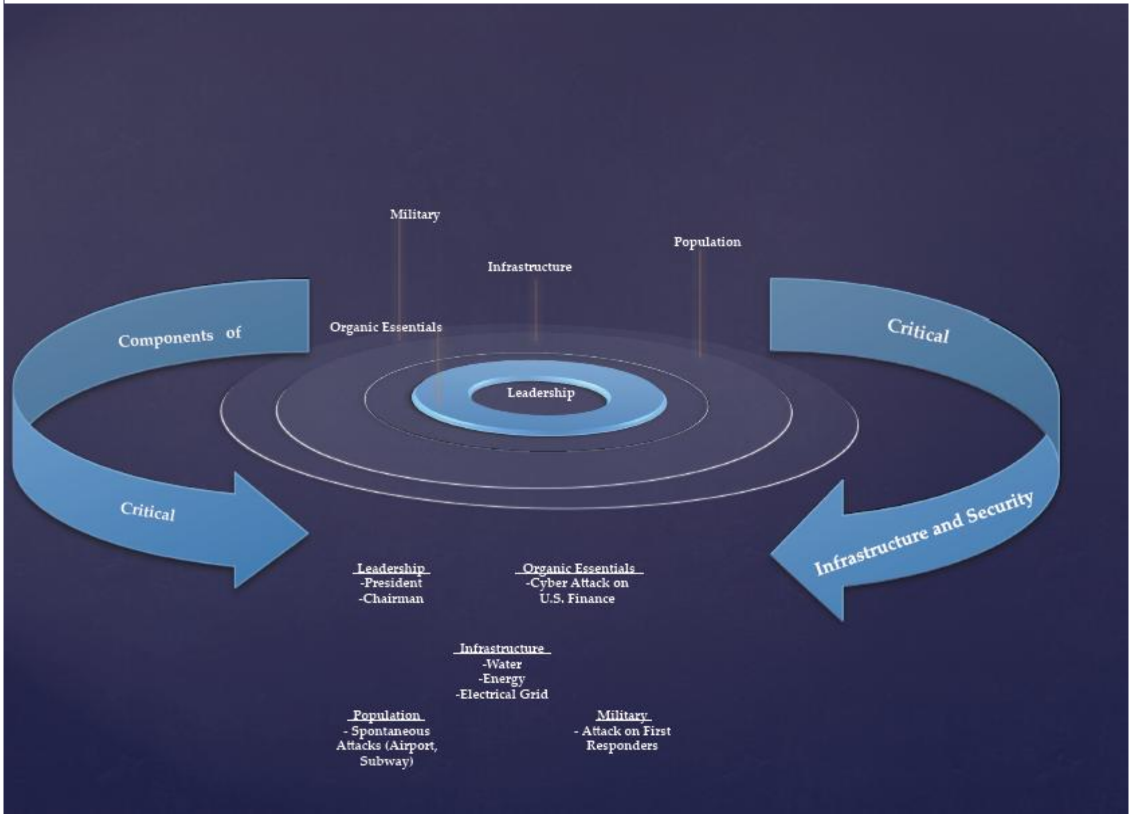
[29] Ibid, 285

Although much more subtle, a baseline of security measures that make it more difficult for the insider to ex-filtrate information is what is ultimately desired. “Creating a baseline of network traffic and systems programs, processes, and connections…greatly assist the ongoing interrogation of the IT environment for breach indicators, because those indicators or deviations from the norm, can be more readily seen”.[30] 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.[31]

CONNECTING THE DOTS

Another illustration that depicts Wardens Five Ring approach is seen in Figure 1. Warden’s approach to this model was meant to include many components of enemy and friendly systems. In order for leadership to be effective organic essentials are needed. These are composed of power production facilities such as electrical grids, nuclear-power plants, and infrastructure correlating to bridges, railways or other key assets.[32] More importantly, this model can be adapted to non-state actors, who may primarily seek to exploit gaps through in security in cyberspace to intrude upon or damage critical infrastructure.

Figure 1. Modified Warden Five Rings Model



[30] Shane Sims, *CIO Update*, “Inside the Cyber Threat Landscape” http://www.cioupdate.com/trends/article.php/3929201/Inside-the-Cyber-Threat-Landscape.htm (March 25, 2011) (accessed 06 Sept 12).

[31] Brian A. Jackson and David R. Frelinger. *Emerging Threats and Security Planning. (2009)*

[32] John A. Warden III “The Enemy As A System,” *Airpower Journal*, Spring 1995

Warden and other air power theorist 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 precise 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.[33] Using a systems approach provides an all-encompassing detailed and dynamic complexity of examining the impact of attacks or exploits against an entire system.

Specifically, Warden's Five Ring Model can be adapted to show a methodology that could be used by an invader, to inflict damage on the U.S. economic system. In review of such a model and its dynamic layered approach, it would take complex planning to affect the inner most ring-the leadership. However, such attack doesn't have to be a precision operation in order to cause damage and to have simultaneous desired effects. Various attack or exploitation methods could be leveraged similar to those during the Estonia conflict in 2007. For instance, As the Russian military mounted its assault on the ground and in the air, a group of Russian nationalist joined in the fray in cyberspace. [34]

These attacks, although denied by Russia on the Georgian public communications, banking institutions, and websites, proved to be a significant psychological victory. With Georgia not being able to disseminate accurate information relative to the ongoing battle to the public, unrest was only added to an already detrimental situation. These attacks illustrated that significant targets could be attacked individually, independent of the systems and have large economic effects. If attacks of such a magnitude were conduct in parallel with other kinetic attacks specifically intended to disrupt of dissuade the economic system of the U.S., the secondary and tertiary effects could be catastrophic.

Ward's model and the above example demonstrate to gain access to the most critical ring-leadership/the command element-would prove relatively difficult. Replacing this leadership structure could be done reasonably soon if additional rings as "Infrastructure" or "Organic essentials" were to breakdown or be severely damaged. Although, challenging, within a strongly interconnected economic environment, intent, and access motivates the will of enemies and the passion to act.

Second, a cyber-attack on U.S. Financial systems and Infrastructure -the second and third rings above- would ripple through the economic system. To date, the Department of Homeland Security, U.S. Secret Service, the Department of Defense, and other organizations are attempting to find nexus points within modern technology to exploit and patch the many security vulnerabilities within cyberspace. Most consequential events and intrusions, by use of cyberspace, require little technical sophistication and can be conducted by outsiders or by inside employees. Such an attack on the finance system or infrastructure, whether primary or secondary, would display many larger-scale events. In turn, consumer confidence in technology, banking, and safeguards may lead to reactionary decisions that could paralyze the finance system.

These are two of many parallel events that can take place within a system that serves to highlight the severe impact of major events. It is not the intent of the two scenarios to present the likely cause or method of a next attack. Nevertheless, security planners must be willing to see cyber, physical security, and critical infrastructure as parts of a system in order to identify threats that can propagate, affecting the entire system. Thus, the Five Ring Model and table previously listed to show

[33] Ibid.

[34] McAfee, "Virtual Criminal Report", 2009.

the simplistic makeup of system analysis and the various methods in which it can be affected must be considered for use.

CONCLUSION

By incorporating a systems approach and conception of parallel attack, security planners may be in a better position to provide more practical indications and warning that reproduce throughout many layers of security. Although Ward's Five Ring Model may not be the most applicable, it can be conformed to aid in homeland security planning. By doing so, security can be better positioned to comprehend the significance of multiple vulnerabilities and likely potential threats to critical infrastructure or key resources that can be intruded upon or destroyed, whether by spontaneous events or dynamically complex events with respect to the overall economy. Warden's model serve to provide security planners with one of the various methodologies to be used to provide a deeper knowledge of system vulnerability and how synchronized, parallel attacks might affect the entire economic system, transcending individual sectors.

The various threat areas identified throughout this research paper demonstrate how the Five Ring Model can be used to look at a system from many diverse lenses. As insider and outsiders seek to find gaps in security systems and a how counterintelligence investigators must be cognizant of the complexity of the opponent and h/her motives. Security planners should also consider the nature of the threat, its intent, and possible levels of access to systems that are tied to critical infrastructure. Finally, Ward's model leveraging a systems analysis framework- can help security planners deduce how the threat is adapting and rapidly evolving, and highlight how security arenas must be positioned to do the same. This approach, in combination with understanding how parallel attacks can cripple multiple levels of security will help security planners more effectively secure the homeland against future attacks.