Title: Governmental Effects upon the Cyber Security Decision Making Cycle
Author: Bruce Norquist
Version: 1.4c, Option 1
Certification: Security Essentials, GSEC
Date: 12 December 2004

ABSTRACT

The purpose of this paper is to consider the direct influence and impact of government agencies on the cybersecurity decision cycle, especially regarding computer system and network critical infrastructure. I am purposely defining and discussing the definitions and fundamental points for cybersecurity, Critical Infrastructure Protection (CIP) and decision-making cycles, and use these items to build a framework or basis for discussing strategic, operational and tactical approaches to cybersecurity.

The Issue

With nearly everything and everyone being connected to the internet directly or indirectly, Are we *cyber secure* in the US? Are we *really* ready to respond to an orchestrated, choreographed cyber attack against infrastructure? Will we *ever really* know when it is happening and will we have the ability to respond aggressively?

In the September issue of Information Security magazine an article's subtitle read: *"Despite heightened post-9/11 security awareness, the U.S. critical infrastructure remains vulnerable to attack"*[1]. From that article we learn, the Financial Services Information Sharing and Analysis Center's (FS-ISAC) view of the 9-11 attacks:

> *Al Qaeda's objectives were clear: Attack rich and visible components of the nation's critical infrastructure to disrupt the U.S. economy, undermine confidence in the monetary system and inflict fresh wounds in the American psyche. The attack could be part of the dreaded "digital Pearl Harbor," a coordinated physical/cyber attack that many have prophesied since the early '90s.*[2]

KEY DEFINITIONS

Cybersecurity

According to the United States General Accounting Office, "*Cybersecurity* refers to the defense against attacks on our information technology infrastructure."[3] Cyber security can be thought of as the combining of network and computer security into a holistic approach to protecting one's IT assets. Cyber security is becoming a more complicated, set of tasks everyday and keeping up with technology seems to be a never-ending task.

[1] Barlas, Stephen and others, "Mission: Critical", *Information Security*, September 2004, URL:http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss467_art974,00.html (29 November 2004)

[2] Barlas, Stephen and others, "Mission: Critical", *Information Security*, September 2004, URL:http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss467_art974,00.html (29 November 2004)

[3] United States. General Accounting Office, *GAO Technical Assessment, Cybersecurity for Critical Infrastructure Protection,* May 2004, GAO-04-321, Page 3. URL: http://www.gao.gov/new.items/d04321.pdf (19 November 2004)

Cyberthreat
In his book, Fundamentals of Network Security, Eric Maiwald defines *threat* as, "An individual who can violate the security of an information system."[4] For the purposes of this discussion, cyber threat or *cyberthreat* refers to the potential for intentional adversary or enemy attack or manipulation against our information technology systems and networks of the critical infrastructure.

Critical Infrastructure
The National Strategy for Homeland Security, uses the USA PATRIOT Act's definition, *critical infrastructures as those "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."*[5]

Within the National Homeland Security Strategy, the critical infrastructure was originally composed of thirteen sectors. The fourteenth, Monuments and Icons was recently added to these original thirteen sectors:

- **Agriculture**
- **Food**
- **Water**
- **Public Health**
- **Emergency Services**
- **Government**
- **Defense Industrial Base**
- **Information and Telecommunications**
- **Energy**
- **Transportation**
- **Banking and Finance**
- **Chemical Industry and Hazardous Materials**
- **Postal and Shipping** [6]

Critical infrastructure and key resources provide the essential services that underpin American society. The nation possesses or regulates numerous key resources, whose exploitation or destruction by terrorists could cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction, or

[4] Maiwald, Eric. Fundamentals of Network Security. McGraw Hill, 2004. Page. 625.
[5] United States. Office of Homeland Security. "The *National Strategy for Homeland Security",* July 16, 2002. URL: http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf (19 November 2004) Page 29.
[6] United States. Office of Homeland Security. *"National Strategy for the Physical Protection of Critical Infrastructures and Key Assets."* February 2003, URL:http://www.dhs.gov/interweb/assetlibrary/Physical_Strategy.pdf, page 6. (19 November 2004)

would profoundly affect our national prestige and morale. Most of these physical assets or key resources are harvested or claimed, enhanced, refined, utilized, tracked, and protected by virtual systems which are networked or stand-alone. According to the DHS and the current administration the fact remains; there is critical infrastructure so vital that its incapacitation, exploitation, or destruction, through terrorist attack, could have a debilitating effect on our nation's security and economic well-being. The virtual or electronic infrastructure, which is interwoven with the physical infrastructure and assets is just as likely and lucrative an enemy target and is also vulnerable.[7]

On September 11, 2001, "the Financial Services Information Sharing and Analysis Center (FS-ISAC) wasted no time alerting its members to the threat, even though the intelligence pointed to a physical attack rather than a cyber-strike. "You can't just look at this as a threat of a physical attack. If you have a physical attack that involves cyber-assets, it's considered a cyberattack," says FS-ISAC chairperson Suzanne Gorman.[8]

Critical Infrastructure Protection – CIP

The National Strategy for Homeland Security and many other official documents do not per se define CIP. But for the purposes of this discussion Critical Infrastructure Protection (*CIP)* is the complete and deliberate effort to safeguard or *protect* those real and virtual assets and their infrastructures with the fullest consideration of cybersecurity and physical security efforts and resources.

In order to reach this standard of *fullest consideration* and become a concerted effort (complete and deliberate), a standard or unified philosophy or methodology must be understood and adopted by the elements involved. This philosophy becomes the foundation of a national strategy for cybersecurity that then can perpetuate and guide operational and tactical decisions and efforts.

FOUNDATIONS OF A NATIONAL STRATEGY FOR CYBERSECURITY

Decision-making Models

The standard decision making cycle can be traced to Col John Boyd, USAF (Ret), who coined the term and developed the concept of the "OODA Loop" (Observation, Orientation, Decision, Action). [9] General Boyd, who invented and made the OODA loop famous, used it to describe the steps a fighter pilot uses to make a decision and

[7] Office of the Press Secretary, White House, "Homeland Security Presidential Directive/Hspd-7. Subject: Critical Infrastructure Identification, Prioritization, and Protection;" December 17, 2003 URL:http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html (4 November 2004)

[8] Stephen Barlas and others, "Mission: Critical", *Information Security*, September 2004, URL:http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss467_art974,00.html (29 November 2004)

[9] "OODA Loop", URL:http://www.mindsim.com/MindSim/Corporate/OODA.html (20 November 2004)

react. “The OODA Loop is now used as a standard description of decision making cycles.“ [10]

For example: one *observes* a enemy aircraft, next s/he *orients* their fighter aircraft, assesses the situation and analyzes possible courses of action, *decides* the best course of action, and *acts* on that decision. “Perhaps most importantly, Boyd was instrumental in explaining and disseminating the concept of "cycle time" and "getting inside the adversary’s decision cycle." [11]

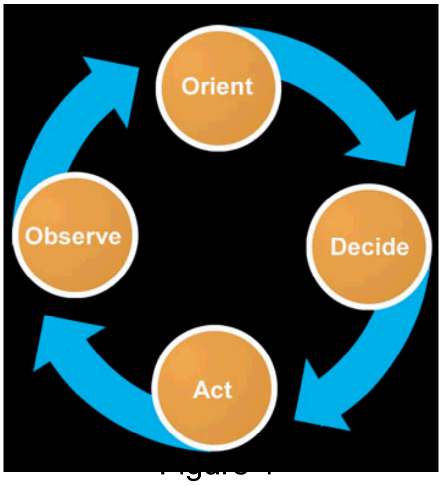


Figure 1

Figure 1, as extracted from the website, http://www.mindsim.com/MindSim/Corporate/OODA.html depicts the basic OODA loop.

Another decision making process, which some may argue is just an updated OODA loop is called, “Lawson's Model”, “was the basis for 3-D visualization and subsequent drill-down … including (1) *sense*, (2) *process*, (3) *compare*, (4) *decide*, and (5) *act*.[13]

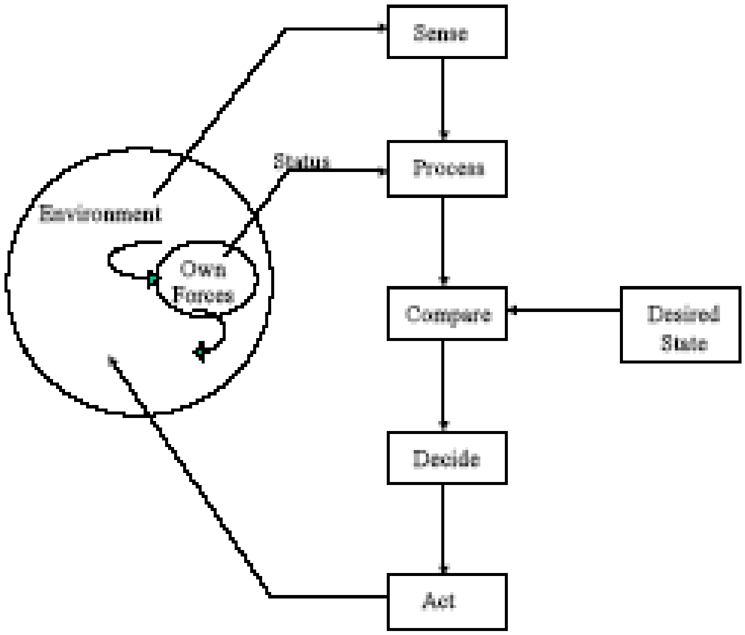
As one call discern from the next figure, Lawson’s Command and Control Model and Boyd’s OODA loop vary only slightly. When comparing *Observe* == *Sense*, *Decide* == *Decision* and *Act* == *Act*. The real similarities are the Decide and Act steps. The difference appears with Boyd’s *Orientation* equating to Lawson’s Process and Compare steps.

[10] “OODA Loop”, URL:http://www.mindsim.com/MindSim/Corporate/OODA.html (20 November 2004)

[11] “OODA Loop”, URL:http://www.mindsim.com/MindSim/Corporate/OODA.html (20 November 2004)

[12] “OODA Loop”, URL:http://www.mindsim.com/MindSim/Corporate/OODA.html (20 November 2004)

[13] [4] Lawson, Joel S. "Naval Tactical C3 Architecture, 1985-1995." *Signal* 33:10 (Aug 1979), pp71-72.



Source: AFCEA Press

Figure 7 Lawson's Command and Control Model

[14]

In a paper presented to the 2002 Command and Control Research and Technology Symposium (CCRTS) at the Naval Postgraduate School, Dr. Hubert D. Callihan, NetSpace Corporation and Mr. John A. Balash, NetSpace Corporation, uses Lawson's model An Experimental 3-D Framework to Support C2 to illustrate an OODA-like loop to meet their needs. More study has reveals "Lawson's Model cited earlier as taken from Allard's *Command and Control and the Common Defense* as shown in **Figure** 7, *Lawson's Command and Control Model* [1]."

> [1] Allard, Kenneth. "Command, Control, and the Common Defense, 2 nd Ed." *National Defense University, Institute for National Strategic Studies,* October 1966, pp154-163.

After reviewing the source document, "Command, Control, and the Common Defense, 2nd Ed." http://www.ndu.edu/inss/books/Books - 1996/Command Control and Common Def - Oct 96/CCCD.pdf it is apparent Lawson based his framework upon Boyd's OODA

[14] Command and Control Research and Technology Symposium (CCRTS) at the Naval Postgraduate School, URL: http://www.dodccrp.org/events/2002/CCRTS_Monterey/Tracks/pdf/105.PDF, pg. 12. (29 November 2004).
[15] Allard, Kenneth. "Command, Control, and the Common Defense, 2nd Ed." *National Defense University, Institute for National Strategic Studies,* October 1966, pp154-163. URL: http://www.ndu.edu/inss/books/Books - 1996/Command Control and Common

loop.[15]

Cybersecurity Decision Cycle Framework

For the purpose of simplicity, the illustration below, figure 2, is the basic OODA loop, which I will overlay with cybersecurity considerations throughout this section, and apply to different echelons or levels of perspective. The following subsections will take this basic OODA decision loop through an evolution process, comparing and contrasting it at the different levels or echelons of view (Tactical, Operational, and Strategic), and discussing how they can affect and impact cyber security. After discussing the framework and each of the echelons, I will present a summary of critical capabilities for each echelon, which supports the need for a unified and succinct National Strategy for Cybersecurity. And, will provide additional information supporting this with the current recommendations provided from other governmental and private sector sources.

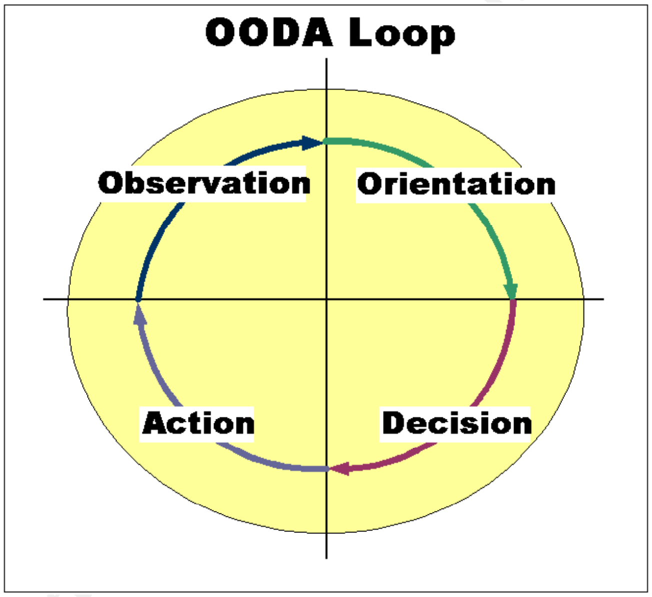


Figure 2

The OODA decision cycle or loop has become one standard method for evaluating tactical decision-making. The same decision cycle can be used for computer network operations (CNO) and computer network defense (CND).

Consistent with acting within an adversary's decision loop, successful cyber security can be thought of as trying to react before or quicker than potential attackers. One method, which can be used to view this challenge, is to think of it as a decision loop, where one wants to perform tasks before an attacker can exploit the vulnerability.

Layered or Echeloned Cybersecurity

When determining governmental impacts it is helpful to view the issue from different

Def - Oct 96/CCCD.pdf (29 November 2004) perspectives and in depth. Using doctrinally accepted echelons of warfare and national security/defense, this means Cybersecurity needs to be viewed from within the three distinct perspectives studied and understood by our policymakers and defenders. Two of the three are more easily defined, and the third, which is more abstract, is the remainder.

- Tactical Level. The tactical level is that of the owner/operator of the critical infrastructure asset. Tactics are implemented and tactical decisions are those made by administrators and operators.
- Strategic Level. The strategic level is that of a national scope and consists of the federal government, its agencies and activities. Strategic actions are limited but strategic decisions made policies, law, and preparation and assistance provided by federal officials and agencies.
- Operational Level. The operational level is that of certain active stakeholders such as state and local governments, regulators, customers, and investors. Those at the operational level have specific interests in the critical infrastructure in question, but do not have rights or authorities to operate the information systems. Actions are again limited, but more extensive than at the Strategic level, and decisions, policies, rules, preparations and assistance are provided by these stakeholders.

Experts recognize there are circumstances where a federal agency is performing at the tactical level, such as operating a power generation facility. In that circumstance it can be considered that the federal government is performing duties at multiple levels.

If one uses the water system, for example, one company's activities' view is at the tactical level. The operational level(s) include state regulators, regional compact, investors and customers. The strategic level or perspective is at the national level, which could include: Department of Energy, Department of Defense, specifically Corps of Engineers operating hydro-electric dams, Department of Homeland Security, and others.

Tactical Level – Operator's Perspective

The owner/operator staff view from the tactical level, and most often make decisions based on their business/organizational needs. Cyber Security's tactical level is best described as the operation of systems and network performed by those people whose job it is to do just that. This cadre of staff is the people who get it done because it is their job and mission. Good professional quality staffs will not abdicate or hand this job over to anyone. However, professionals will accept advice from other professionals when presented in the non-hostile, non-threatening manner.

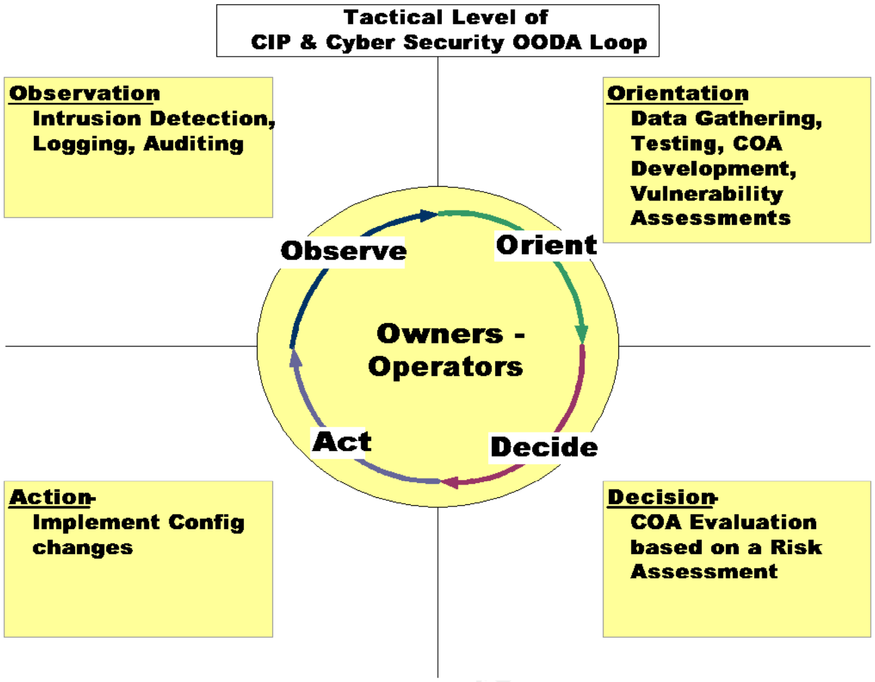

Tactical Level of
CIP & Cyber Security OODA Loop
Observation
Intrusion Detection, Logging, Auditing
Orientation
Data Gathering, Testing, COA Development, Vulnerability Assessments
Observe
Orient
Owners - Operators
Act
Decide
Action
Implement Config changes
Decision
COA Evaluation based on a Risk Assessment

Figure 3

This chart lists key aspects of the operators and administrators OODA perspective:

Tactical Observation	**Tactical Orientation**
System monitoring – to detect anomalies, and attacks	Researching anomalies
Observing current network and system configurations	Gathering information on system and network configuration
Observing known vulnerabilities within a configuration	Gathering information as to whether known vulnerabilities are being used intentionally for use within the architecture
	Prototyping action, whether making this change will break anything else.
Tactical Decision	**Tactical Action**
Decisions based on a risk assessment, as to what is the risk, does this risk affect the IT in use; will the corrective action or mitigation correct the vulnerability and not impact anything else.	Actions taken as the result of well-researched decisions.

Operational Level – Active Stakeholders Perspective

Those active stakeholders, primarily policymakers and regulators but also including the customer base and investors, view from the operational level. The scope involved at the operational level is that which is more than one company's cyber security concerns, but does not include the entire sector.

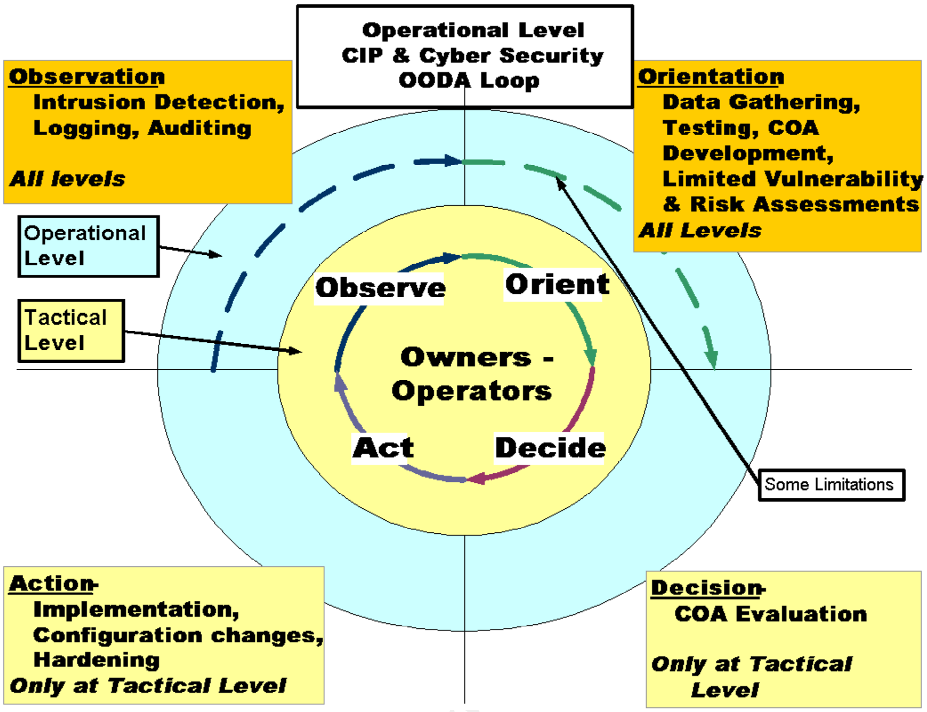


Figure 4

This chart lists key aspects of operational or stakeholders' OODA perspective:

Operational Observation	**Operational Orientation**
Receiving results of system monitoring, to see anomalies, and attacks	Gathering more information on system and network configuration
Receiving results of current network and system configurations	Gathering information as to whether known vulnerabilities are being used intentionally for use within the architecture
Receiving results of known vulnerabilities within a configuration	Prototyping action, where a "patch" is applied, can be used to attain foundational information – whether making this change will break anything else
Operational Decision	**Operational Action**
Decision-making at the operational level does not exist; since the operational level does not own or operate the assets being secured, there is limited ability to act or compel action.	Actions at the operational level are limited to the powers of coercion, regulations and statutory guidance.
Decisions need to be based on a risk assessment, as to what is the risk, does this risk affect the IT in use, will the corrective action or mitigation correct the vulnerability and not impact anything else.	A regulator may fine non-compliance, but cannot actually make system changes.

Strategic Level OODA Perspective – National Government
The strategic level can be thought as the federal government and its' various agencies. The scope involved at the strategic level is more than one company's cyber security concerns, with regional and especially national concerns for the entire sector.

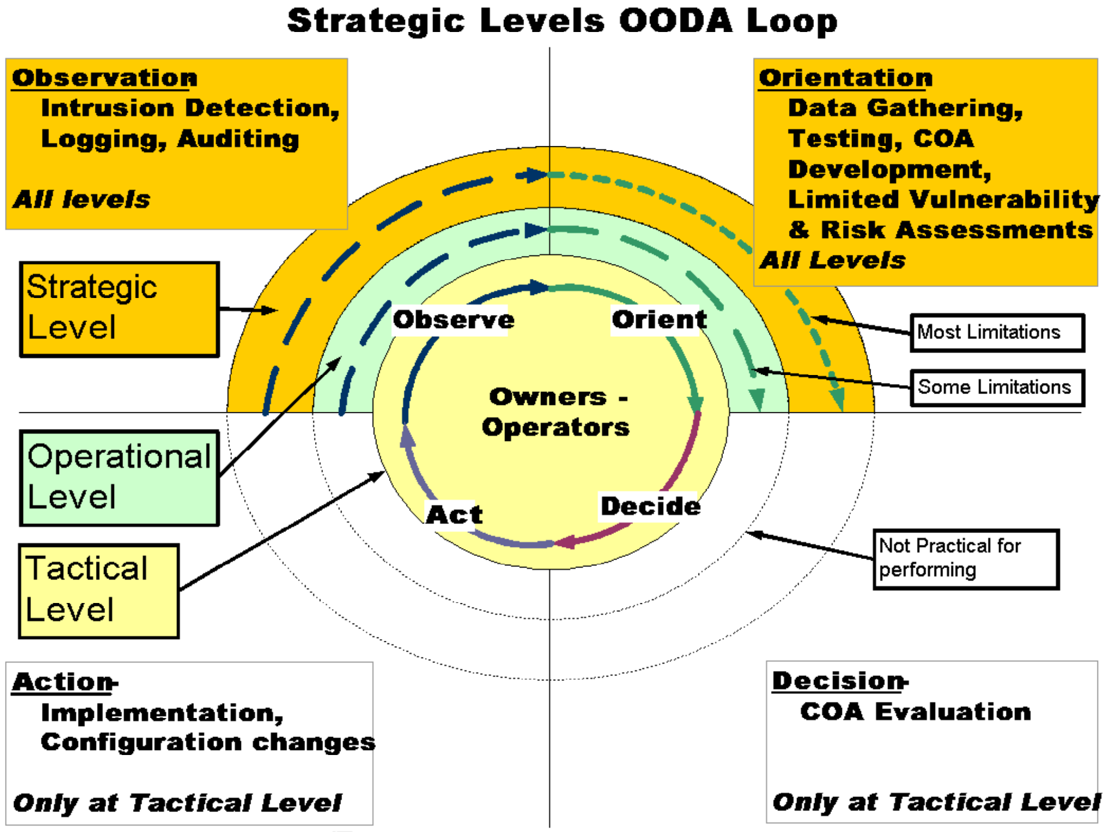


Figure 5

As depicted in the figure above, in the Decision and Action steps, again the operational level is not shaded, and the strategic level in added. It still remains highly unlikely that the federal government would make any decisions or take any direct actions in respect to Cyber Security. However, the observation and orientation steps do present a potential for federal interaction and enforcement, which will be discussed later.

Strategic Observation	**Strategic Orientation**
Strategic Observation occurs when system monitoring, detection of anomalies, and attacks are correlated and predictive analysis is performed	Strategic Orientation occurs when predictive attack patterns and trends are forecast.
Strategic Decision	**Strategic Action**
There is no such thing as a Strategic Decision in Cyber Security.	There is no such thing as a Strategic Action in Cyber Security.

SUMMARY OF CRITICAL CAPABILITIES & SUPPORTING RECOMMENDATIONS

Tactical Capabilities

Standardization of observation, orientation and decision-making will greatly enhance the robustness of Cyber Security. Increasing the speed of action, like the other steps at the tactical level is primarily dictated by the available resources and the action required.

Operational Capabilities

Viable operational capabilities, which are only apparent in the observation and orientation steps, require standardization and cooperation from the tactical level (the owners and operators).

Strategic Observation and Orientation

Just like the operational capabilities, the only steps viable at the strategic level are the observation and orientation steps. For strategic observation and orientation to be effective, these are the imperatives:

- Obtaining the data from owner/operators
- Identify and profile attacks trends
- Standardized vulnerability assessment methodologies
- Standardized red teaming / penetration testing
- Correlation of attacks or penetrations across the entire critical infrastructure and by CI sectors and with governmental information

Recommendations

There have been numerous studies, workshops, recommendations and plans for improving cybersecurity for CIP. The GAO report, Cybersecurity for CIP, recognized several projects. The basis to most of these recommendations centers on cooperation with the private sector and can only exist in a public-private partnership. *"With about 85 percent of the nation's critical infrastructures owned and operated by the private sector, public-private partnership is crucial for successful critical infrastructure protection*."[16]

For example, in December of 2003, the Cyber Conflict Studies Association (CCSA) and the Center for Technology and National Security Policy, National Defense University, held a workshop, COMPLEXITIES and Critical Infrastructure Vulnerabilities. Some of the select recommendations are:

Policy – must be resolved as a national mandate requiring action from senior leaders in national security and homeland defense

- Develop appropriate response decision-making approaches and options in

[16] United States. General Accounting Office, *GAO Technical Assessment, Cybersecurity for Critical Infrastructure Protection,* May 2004, GAO-04-321, Page 6. URL: http://www.gao.gov/new.items/d04321.pdf (19 November 2004)

the event of cyber attacks

- o Develop mechanisms for orchestrating joint government and private entities funding necessary to implement more effective cyber defense policies

Strategy – affects national planning, protection, or oversight activities

- o Develop a National Cyber Red Team and strong command and control functions for Cyber conflict.

Tactics – affects operation and management of infrastructure

- o Develop a methodology and technology approaches to assess that when critical infrastructure(s) is (are) under attack

Research – requires further study and funding

- o Studies in the applications of traffic analysis and other techniques to identify internal and external threats and threat agents[17]

CHALLENGES TO A UNIFIED STRATEGY & STANDARDIZATION

Obtaining the data from owner/operators has been the most difficult task, which all of the other imperatives rely upon. Without reliable data from the owners and operators, no other strategic and operational level activities will significantly improve cyber security for the critical infrastructure.

The first active step in this process is then, to gather the needed data. This could be accomplished by collecting data, such as intrusion detection systems (IDS) and firewall logs. The remaining imperatives such as predictive attack warnings, and correlations across the national require a data repository and data mining analytics commercially available.

But an initial first step, imperative to the acceptance of a unified philosophy and methodologies of a National Strategy for Cybersecurity is to gain confidence. In our free-market society we value a less intrusive government and consumer confidence drives the markets. Here, the credibility of the effort would have to be demonstrated and the confidence campaign won in order to gain the fullest cooperation of the private sector. We first have to get buy-in*,* and this entails marketing value to the stakeholders and owner/operators for their acceptance of this Strategy. A backing by the administration, the states, and an Office of Homeland's *seal of approval* would all aid in achieving this end.

EXAMPLE CAPABILITY

"Observation" Step Provides Cyber Threats

So after reviewing the tactical, operational and strategic OODA loops, the next question is what does one of these capabilities look like. Taking the "observation" step and putting it into conventionally understood vernacular, an "observation capability" is

[17] **Complexity and Critical Infrastructure Vulnerabilities,** The Center for Technology and National Security Policy, National Defense University, pages 3-4. http://www.ndu.edu/ctnsp/Complexity Book.pdf (19 November 2004)

needed which can:

- Observe cyber threat activity against the critical infrastructure
- Analyze these threats against the governments, corporations and industries
- Generate predictive models of strategic threat profiles, signatures and trends within and across the infrastructure sectors
- Perform cross-sector analysis and geographic centered correlations
- Perform cross network attack correlation and aggregation, both among individual infrastructure areas and across different infrastructure sectors
- Focus on outside threats to the perimeter, and not focused on inside a network

Characteristics

This capability or activity spans multiple governmental, political and legal jurisdictions, and is focused on the outside threat. Therefore, the case is made that this activity:

- Requires a trusted agent or trusted activity
- Options for conduct include: Not-For-Profit, Non-Profit and Government activities
- Responsive and timely
- Provide customer anonymity
- No-cost, Low-cost or Government subsidized service
- Widespread participation
- Daily processing

The desired end state is to provide a service, which can collectively improve cybersecurity of the entire critical infrastructure.

Implementation Steps:

1. A critical infrastructure "client" is identified and the Cyber Threats service is presented
2. Cyber Threats service is presented to critical infrastructure owners/operators
3. Non-disclosure agreements and memorandums of agreement are negotiated and signed by "client" and service
4. Reliable and trusted connectivity is enabled
5. Logs are forwarded to service
6. Proprietary or company identifying information is removed (data is redacted)
7. Processed logs loaded into a database
8. Reports generated
9. Comparative analysis is made:
   - To similar companies, within the same sector - e.g a power-generating company's threat activity is compared to another
   - Geographic correlations across all sectors – e.g. attacks are compared between the power-generating companies, local government, telecommunications, ….all within the same geographic region, or state
   - Correlations between federal systems, e.g attacks upon DoD infrastructure, other federal systems
10. Generate a customized reports, with predictive cyber threats based upon analysis and correlations from the database
11. Distribute reports

Operational Example

The only working example of a program with some or all of these characteristics can be found within the Foreign Military Studies Office (FMSO) of Training and Doctrine Command (TRADOC), United States Army. Within FMSO, there is an activity called Homeland Infrastructure Security Threats Office (HISTO) focusing on full spectrum threats (physical and cyber) to the critical infrastructure. Embedded within HISTO is the Critical Infrastructure Assurance Program – Cyber Threat (CIAP-CT). [18]

Currently, CIAP-CT's website is not available, so the program information was gathered through interviews and emails. During the discussions there are numerous federal and state agencies who are quite surprised by the CIAP-CT existence and its' successful four year history. These same agencies that are mandated to generate cyber threats and have yet to get private sector participation are stunned that CIAP-CT has been doing just that for years.

The primary reasons for CIAP-CT's success has been its' relationship with the National Guard vulnerability assessment teams, and CIAP-CT gives something back to participating companies.

As with all military organizations, they are built on a mission statement, which outlines the parameters the organization should operate. The CIAP-CT mission statement reads as follows:

> The Critical Infrastructure Assurance Office – Cyber Threats (CIAP-CT) is to continually conduct computer network and cyber threat analysis, develop doctrine, coordinate and support exercises, develop and advance policies, procedures, standards and maintain a knowledge base on the cyber threats to the public and privately owned critical infrastructure sectors, which support DoD's power projection capabilities ("outside-the-fence") to minimize the effects of catastrophic events on the public-private-interagency sectors. CIAP-CT is to provide military assistance to civil authorities, as directed by the President or the Secretary of Defense. [19]

CIAP-CT Products

From the interview with the CIAP-CT director and subsequent emails, the products from CIAP-CT should be considered:

- Single nationwide repository (data warehouse) of the actual cyber attacks against the private corporations comprising the critical infrastructure
- Ongoing analysis of asymmetric cyber threats by individual company, sector, and across sectors against the critical infrastructure
- Reports generated for participating customers (monthly)
- Models of strategic threat profiles, signatures, and trends within and across

[18] MAJ Jeff Newhard, CIAP-CT Director, US Army, interview by author, Fort Leavenworth, KS, 1 December 2004.

[19] Email from MAJ Jeff Newhard, CIAP-CT Director, US Army. 2 December 2004.

infrastructure sectors

CIAP-CT Challenges:

Resources and staff. Staffing is the most significant challenge. CIAP-CT has primarily used Army Reservists and Army National Guardsmen for the analysis and report generation steps. Due to the ongoing operations, access to reservists and guardsmen has been eliminated.

Scalability. Although CIAP-CT has been operating for four (4) years, it is still a labor-intensive operation. The technology and means exist to automate the reporting and analysis processes, but additional resources and staff is needed to deliver more than monthly reports. In other words, in order for CIAP-CT to be responsive enough to assist in detecting and alerting customers about a zero-day exploit, more resources are required.

Benefits

- The Homeland Defense/Security agencies can better ensure the reliability of the critical infrastructures that support installations, force projection assets, and ultimately economic stability
- Private Industry receives the only predictive threat assessment with cost effective methodologies to effectively assess threat vulnerabilities without jeopardizing the privacy required to compete in today's economy.
- No other entity has successfully combined cyber attacks over the entire critical infrastructure and provides Cyber Threat warnings unique to companies

Example Summary

The CIAP-CT program is an example of a strategic, federal activity, which operates in the "Observation" step of the OODA loop. CIAP-CT does not and cannot direct decisions or actions, but pulls together cyber threats across the entire infrastructure.

CONCLUSION

The OODA loop provides a logical and detailed perspective on viewing Cyber Security. The framework attempts to describe the different functional levels (Tactical, Operational, and Strategic) and can spur discussions about the different scopes or spans of government at the levels.

It is imperative the involved entities understand what can reasonably be expected of government and by government. The role of our government being to "*promote the general welfare*" while providing secure and defensible way of life and maintaining a separation from direct involvement/competition in commerce. This is a mandate for governmental focus and efforts in areas it can affect, without too much intrusion – the provision and reinforcement of infrastructure accomplishes this end. In this is the way the US Federal government does recognize what aspects of cyber defense should be and can be provided within the scope of the law, and is actively engaged in supporting commerce and free enterprise. Additionally, this reinforces in the public sector that the actions are not forceful or compelling, nor are attempts or efforts made to install/implement/configure a *certain decided* feature or software on every system.

REFERENCES

Barlas, Stephen and others, “Mission: Critical”, *Information Security*, September 2004, URL:http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss467_art974,00.html (29 November 2004)

United States. General Accounting Office, *GAO Technical Assessment, Cybersecurity for Critical Infrastructure Protection,* May 2004, GAO-04-321, Page 3. URL: http://www.gao.gov/new.items/d04321.pdf (19 November 2004)

Maiwald, Eric. Fundamentals of Network Security. McGraw Hill, 2004. Page. 625.

United States. Office of Homeland Security. “The *National Strategy for Homeland Security”,* July 16, 2002. URL: http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf (19 November 2004) Page 29.

United States. Office of Homeland Security. *“National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.”* February 2003, URL:http://www.dhs.gov/interweb/assetlibrary/Physical_Strategy.pdf, page 6. (19 November 2004)

United States. Office of the Press Secretary, White House. “Homeland Security Presidential Directive/Hspd-7. Subject: Critical Infrastructure Identification, Prioritization, and Protection;” December 17, 2003 URL:http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html (4 November 2004)

“OODA Loop”, URL:http://www.mindsim.com/MindSim/Corporate/OODA.html (20 November 2004)

[4] Lawson, Joel S. "Naval Tactical C3 Architecture, 1985-1995." *Signal* 33:10 (Aug 1979), pp71-72.

Command and Control Research and Technology Symposium (CCRTS) at the Naval Postgraduate School, URL: http://www.dodccrp.org/events/2002/CCRTS_Monterey/Tracks/pdf/105.PDF, pg. 12. (29 November 2004).

Allard, Kenneth. "Command, Control, and the Common Defense, 2nd Ed." *National Defense University, Institute for National Strategic Studies,* October 1966, pp154-163.

URL: http://www.ndu.edu/inss/books/Books - 1996/Command Control and Common Def - Oct 96/CCCD.pdf (29 November 2004)

The Center for Technology and National Security Policy, “Complexity and Critical Infrastructure Vulnerabilities”, National Defense University, pages 3-4. http://www.ndu.edu/ctnsp/Complexity Book.pdf (19 November 2004)

Major Jeffrey Newhard, CIAP-CT Director, US Army, interview by author, Fort Leavenworth, KS, 1 December 2004.

MAJ Jeff Newhard, CIAP-CT Director, US Army. email to author, 2 December 2004.