Proceedings of the 8th Colloquium for
Information Systems Security Education
West Point, NY June 2004

Infrastructure Assurance: The New "I" in Information Assurance Education

Aaron J. Ferguson, Ph.D., CISSP, Member, IEEE

Abstract – *The blackout during the summer of 2003 proved that our critical infrastructures, e.g., power grid, are vulnerable! According to experts in the Department of Homeland Security (DHS), the likelihood of a blended attack---physical and cyber—on our nation is relatively high. This paper makes the case for educators and curriculum developers to broaden current Information Assurance –focused curriculum, concepts and pedagogies to include" Infrastructure Assurance." This paper will do this by: (1) describing and discussing the notion of convergence theory--the next attack will be a blended attack of physical and cyber dimensions; (2) identifying the components that comprise the U.S Critical Infrastructure;(3) discussing the notion of "Infrastructure Assurance" and its role in current Information Assurance curriculum; and (4) using a regional water supply system scenario, provide a framework for developing a Critical Infrastructure Protection (CIP) strategy framework and pedagogically integrating Infrastructure Assurance into existing Information Assurance curriculum.*

Index terms – Information Assurance, Infrastructure Assurance, Cyber Warfare Convergence Theory, Bloom's Taxonomy, Critical Infrastructure Protection (CIP)

I. CYBER-WARFARE CONVERGENCE THEORY

According to the National Strategy to Secure Cyberspace, by exploiting vulnerabilities in our cyber systems, an organized cyber attack may endanger the security of our Nation's critical infrastructures.[1] A United States General Accounting Office report titled, "Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors," predict that the next attack on the United States will be a blended attack—a combination of a physical and a cyber attack on our critical infrastructure components[2]. The effects of a blended attack include slowing or complicating the response to a physical attack. The report states that Federal efforts to protect our nation's critical infrastructures have had mixed progress. In response to these systemic deficiencies, in 1998, President Bill Clinton established Presidential Decision Directive (PDD) 63. The PDD 63 calls for a range of actions to improve the nation's ability to protect our critical infrastructure against cyber, physical, or blended attacks. Dario Forte, security advisor to the European Electronic Crimes Task Force, submits that ability to launch a coordinated attack physically and virtually—is about five years away. This theory, now known in many circles as convergence theory, is rapidly becoming the wakeup-call for improving the security posture of our nation's infrastructure.

These incidents indicate that, in addition to educating and training our Information Security professionals, we must address these issues in our nation's undergraduate classrooms! In the sections that follow, a framework for addressing these issues from a pedagogical perspective will be discussed. The next section will define critical infrastructures and discuss their attributes.

II. WHAT IS US CRITICAL INFRASTRUCTURE?

The State Infrastructure Advisory Committee, Executive Order 13010, signed by former President Clinton in 1996, defines critical infrastructure as:

"Those systems and assets which are so vital to the United States, that the incapacity of such systems and assets would have a debilitating impact on the country's ability to function, or would have a deleterious effect on the country's morale."[3]

The GAO report mentioned earlier, reports that private-sector entities control over 80% of our nation's critical infrastructures. Moreover, at least 50% of these entities rely on networks and the Internet for maintaining an adequate level of operational efficiency and reliability. Because networks have become pervasive throughout the infrastructure backbone, we are subject to an increased level of cyber threat. According to Paula Scalingi, director of the Department of Energy's Critical Infrastructure Protection Office, "the terrorists in the Sept. 11 event had the patience to plan [and] the foresight and the understanding of the infrastructure that could be used to simultaneously or sequentially disrupt the infrastructure electronically and that could cause a major regional failure in this country."

A vast majority of the public can not identify the components of the United States' Critical Infrastructure (CI). The United States' CI consists of the following components[4]:

- **Electrical Power** – The Nation's power grid including the sub-stations that support it.
- **Gas and Oil production, Storage, and Delivery** - From the Alaska pipeline to oil refineries to natural gas distribution.

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

- **Telecommunications** - Includes Internet, cable, cellular, telephone, satellite, and any other medium that connects systems together.
- **Banking and Finance** - The movement of trillions of dollars of virtual money through brokerages and banks over computer wires and networks.
- **Water Supply Systems** - Computers perform the water supply and waste disposal management.
- **Transportation** - Ground deliveries, air traffic control, and trains. All play a huge role in delivering food and materials to businesses, hospitals and other tourism-dependent entities.
- **Emergency Service** - 911, fire and police departments, rescue units all rely upon the communications networks to do their job with speed and efficiency.
- **Government Operations** – This includes law enforcement and general provision of municipal services. The government has to make sure that during an attack; the government survives and maintains control of the city, state, or country.

The current focus of Information Assurance programs at the undergraduate and graduate level is on Local Area Networks (LANs) and to some degree, Wide Area Networks (WANs)[5]. These programs should broaden the perspective and look at the network from an "Infrastructure Assurance" perspective. Information Assurance is an enabling component of Infrastructure Assurance. Before the components of the infrastructure are examined for a security posture assessment, it is important to understand who has authority over each component and how these authorities communicate with each other. A key component of Infrastructure Assurance is the ability to communicate effectively between and among infrastructure stakeholders. The next section will define Infrastructure Assurance and discuss its attributes.

III. WHO IS IN CHARGE OF OUR CRITICAL INFRASTRUCTURE?

Even though the Federal government provides a leadership role over critical infrastructure components, these components are led by different sectors of the government. President Bush felt that this leadership should be centralized and coordinated. The Bush administration, under the Homeland Security Act of 2002 established the Department of Homeland Security (DHS). The DHS is responsible for: (1) developing a national critical infrastructure plan for securing critical infrastructure resources; (2) recommending security measures for protecting these resources;, and (3) sharing infrastructure security posture information with other infrastructure sector owners[6]. Table 1 shows the lead agency responsibility. The DHS is comprised of over 20 agencies with different ways of doing business. With differing degrees of responsibility among sectors, it is no wonder that a comprehensive security strategy is not in place and security posture development progress is slow.

Table 1. CI Lead Agencies and Sectors

Lead Agency	Sectors
Homeland Security	Information and Telecommunications, Transportation, Postal and Shipping, Emergency Services, Continuity of Government
Treasury	Banking and Finance
Health and Human Services	Public Health, Food (except meat and poultry)
Energy	Electrical Power, Oil and Gas Production and Storage
Environmental Protection Agency	Water, Chemical Industry and Hazardous Materials
Agriculture	Food (meat and poultry)
Defense	Defense Industrial Base

Source: National Strategy for Homeland Security and PDD 63

The main issue is getting students to consider all of the components of an Infrastructure--physical and organizational as one strategy does not fit all. One of the key responsibilities of DHS is to facilitate information sharing with other commercial, civil and federal agencies. A report by the Markle Foundation Task Force reports that information sharing between DHS and other agencies is extremely limited[7]. The next section will unpack the multiple characteristics of Infrastructure Assurance.

IV. ATTRIBUTES OF INFRASTRUCTURE ASSURANCE

According to the National Security Agency, Information Assurance can be defined as:

"The use of information and operations that protect and defend information, information systems, and networks by ensuring their availability, integrity, authentication, confidentiality, nonrepudiation, and continuity in the event of a cyber or physical attack.

Adapting the National Security Agency's definition of Information Assurance, Infrastructure Assurance can be defined as:

"The use of information and operations that protect and defend critical infrastructure information, information systems, and the structures they reside in and on by ensuring their availability, integrity, authentication, confidentiality, nonrepudiation, and continuity in the event of a blended attack."

Like Information Assurance, Infrastructure Assurance has the following critical attributes: (1) its context sensitive; (2) its dynamic; and (3) its multidisciplinary. These three

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

attributes can also describe an adversary[8]. As such, any CIP strategy should contain these attributes.

Infrastructure Assurance is context sensitive--different critical infrastructure components have different threat models. As such, from a pedagogical perspective, students should be able to demonstrate conceptual understanding of threats, vulnerabilities, and risks in multiple contexts—cyber and physical. These threats models will drive development of a critical infrastructure protection strategy framework.

Infrastructure Assurance is dynamic because technology changes every 18 months and new vulnerabilities are discovered everyday. As more of our CI service providers, e.g., power companies, water suppliers, do maintenance and monitoring over the Internet, the adversary is watching. Trying to maintain a robust security posture is a full time job that often requires dynamic information system protection strategies. As such, when used in a critical infrastructure context, educators and students have to stay abreast of the security challenges that new technology and technology strategies inevitably bring along.

Infrastructure Assurance is multidisciplinary. It is pervasive across environmental, financial, social, and mathematical disciplines. Students have to understand that Infrastructure Assurance knows no boundaries! Being able to assess policy and technology impacts in a variety of environments is essential to developing Infrastructure Assurance strategies.

It is important to note that Information Assurance within the context of Infrastructure Assurance has a fiscal component that often drives protection strategy. One example is the power industry. The need to maximize profits at the risk of safety and service can transcend the need to protect our data. The Northeast region power outage is a prime example of this. Companies that control our nation's power grid are in a low margin business. The leaders of these organizations have to decide to either replace decaying infrastructure, which can be expensive, especially if the current infrastructure is functional or put security in to protect my information. In most cases, the later choice is the most unpopular.

The next several sections will provide examples of how vulnerable our critical infrastructures are. The student needs to understand the tradeoffs between security and convenience within the context of our critical infrastructures and across multiple disciplines.

V. SECURITY POSTURE OF U.S. CRITICAL INFRASTRUCTURE

According to the National Security Agency, foreign governments already have or are developing computer attack capabilities, and potential adversaries are developing a body of knowledge about U.S. systems and methods to attack these systems. In early 2002, information on computerized water systems was recently discovered on computers found in Al Qaeda camps in Afghanistan[9]. Also of note is the fact that the National Security Agency's "Eligible Receiver" exercise in 1997 demonstrated how vulnerable Department of Defense (DoD) systems are. While the Internet does provide some degree of efficiency and reduction in operation and maintenance costs, it does introduce substantial risk to networks and the information that resides in/on them. The next five operations security-related examples will illustrate why.

Example 1: Web audits have found descriptions of physical locations of Heating, Ventilation, and Air Conditioning (HVAC) backup facilities, the number of people working there as well as detailed information about how the HVAC system is configured.[10] Lesson learned: students need to know and understand what good operations security practice looks like!

Example 2: Verton (2003) describes the American Airlines wireless initiative that made them one of the first airlines in the country to install wireless roving agents and passenger check-in systems. Even though this technology made the customer's experience more efficient, the lack of basic security technologies like encryption, illuminated American Airlines' vulnerability to a wireless attack. For example, all mobile computers were integrated into the baggage check system, reservation system, aircraft maintenance databases, and numerous other airline networks. There was nothing to stop a hacker from sniffing out the airline IP addresses and causing life-threatening havoc. Imagine if a terrorist could modify data in the reservation system changing the names of suspected terrorists. Lesson learned: students need to understand threats from a system level vice the system component level.

Example 3: Today, anyone performing a basic "*Google*" search can locate the exact location of every nuclear reactor in the United States and other countries. This is notable because: (a) Alexander Breeding, in his August 2003 article titled *Sensitive but Unclassified Information: A Threat to Physical Security*, found the same information and today, the information is still there; and (b) the National Infrastructure Protection Center (NIPC) has made several requests for the International Safety Center to put this information in a place where only those with a "need-to-know" can get to it.[11] Breeding not only found

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

the exact location of these reactors, he also pinpointed their locations using a Global Positioning System (GPS) system and the web. Breeding went a step further by locating all routes of travel from various states, via highway and rail, to the Nevada nuclear waste facility in Yucca Mountain. Looking at protections of our networks without revisiting our public information access strategy will only increase the likelihood and frequency of a blended attack.

Example 4: Breeding also found a map of every electrical power generating station in California. This map was broken out by county, and listed each plant, its location, and the type of power plant it was (e.g., biomass, coal, digester gas, nuclear, etc.)[12]. He also found a map for detailing California's major electric transmission lines.[13] Students should understand how to balance the need to access information with determining who needs to access certain information.

Example 5: Several months ago, a recent article in the Washington Post entitled "Dissertation Could Be Security Threat" by Laura Blumenfield described the work of a George Mason University graduate student as so compelling that government authorities want to suppress it. Using information found out on the web, this graduate student was able to map every business and industrial sector in the American economy, layering on top the fiber-optic network that connects them.[14] In the dissertation, the student could click on any bank in New York City's five boroughs and determine who has communication lines running into and out of the bank and where. He was able to zoom in on the city of Baltimore and find the choke point for trucking warehouses.

The first step in securing our critical infrastructure is establishing a judicious and consistent process for determining what information should be accessible to the public and what should not. Having students write an information classification policy could help students develop a critical infrastructure information protection strategy.

VI. WHAT SHOULD WE DO ABOUT IT IN THE CLASSROOM?

Teaching Infrastructure Assurance as part of an existing curriculum is not trivial. It takes longer than an academic year to master the art of developing, coordinating, and implementing a Critical Infrastructure Protection strategy framework. Whatever approach is used should provide the opportunity for students to demonstrate the six levels of Bloom's taxonomy (see Figure 1 below).

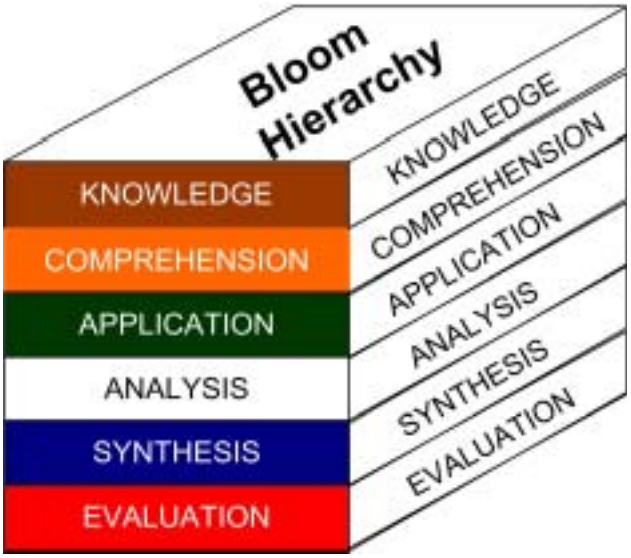


Figure 1 IA taxonomy

Bloom's taxonomy is one of several models that characterize student-learning models. It is used here to make a point about the need to make any information and/or infrastructure assurance concept(s) educationally relevant; not to advocate the use of Bloom's taxonomy as a silver bullet for pedagogical strategy.

In Bloom's taxonomy, there are six levels of competency: (1) knowledge, (2) comprehension, (3) application, (4) analysis, (5) synthesis, and (6) evaluation[15]. The first level of competency — knowledge — is focused on having the student list, define, tell, describe, and name concepts. This level of knowledge is about identifying terms and concepts. The second level of competency—comprehension—creates a deeper level of abstraction--the student is now asked to interpret, summarize, discuss, and predict. This layer forces the student to demonstrate a higher level of conceptual understanding. The third layer—application—is about making use of the knowledge, i.e., demonstrate, modify, operate, and produce. The comprehension of the knowledge is demonstrated during the application layer. In the fourth layer—analysis—the student is asked to explain, extrapolate to multiple contexts, and make connections. In layer five—synthesis—the student should be able to explain concepts in multiple contexts. In the final layer—evaluation—the student should be able to demonstrate a level of critical thinking beyond the synthesis phase.

These six levels of competency will lay the groundwork for development and implementation of a six-phase CIP strategy framework. This strategy will consist of: (1) identification of CI assets; (2) security requirement development and analysis of these CI assets; (3) threat and vulnerability analysis; (4) Risk analysis; (5)

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

development of a CIP strategy; and (6) implementation of this strategy. In order to lay the foundation for this strategy, consider the following regional water supply based scenario:

The Susquehanna River Basin (SRB) is one of the largest interstate waterways in the United States. It includes the tributaries and terminal points of the Susquehanna River, which flow through New York, Maryland, and Pennsylvania. The SRB serves numerous industries, residential regions, and a local nuclear power plant. Water allocation is performed through computerized allocation models that are connected (via the Internet) to other regional river basins across the country. Several factors go into SRB water allocation models. They include: (1) degree of environmental damage prevention; specifically, toxic dumping and nutrient and sediment loads; (2) probability of delivery; (3) availability; specifically for nuclear power generators, commercial food industries and hospitals; and (4) average salinity levels. Your task is to develop a strategy for a CIP framework for the SRB.

As a side note: a map of the SRB regional layout is available on the Internet (Figure 2 below) [16]. This map would aid an adversary in profiling pressure points of the water supply system

Figure 2: SRBC Nutrient and Sediment Loads

A. IDENTIFICATION OF CI ASSETS

Identifying, defining, and describing CI assets are the first steps in developing a CIP strategy. This step is implementing the top layer—knowledge—of the Bloom Hierarchy. Students should be able to perform these actions for multiple critical infrastructure components and assess similarities and contrasts.

In addition to being able to identify, define, and describe, the student should be able to answer the following Critical Infrastructure asset questions: (1) who controls it? Is it a sub-contractor? (2) Who is responsible for it? (3) Who uses it? and (4) How is it used?[17] Merely identifying CI assets with no knowledge/insight of/into the aforementioned questions will limit the utility of any CIP strategy.

B. SECURITY REQUIREMENTS

Identifying, defining, and describing critical infrastructure security requirements of the identified critical assets are the next phase in developing a CIP strategy framework. Alberts and Dorofee (2003) discuss a very important issue to consider after the identification phase—security requirement prioritization. For example, senior managers may consider confidentiality more important than data integrity. Staff members may consider availability more important than confidentiality; and customers may see availability more important than both confidentiality and unauthorized access. The student should have the opportunity to discuss and provide rationale for each requirement. In the SRB example, senior management may consider data integrity more important than confidentiality.

As the students perform this exercise, they should consider which assets and will have a large adverse impact on the infrastructure component in all of the following scenarios:

- **Unauthorized Disclosure of Sensitive Information and Unauthorized Access**: The student should understand when data integrity might be more important than data confidentiality. As CIP components are identified, they should assess whether the right people have access to the data they should have access d. In the case of the SRB, can someone inadvertently change salinity levels or nuclear power generation provision levels? Are these auditable events? Moreover, they should think about the potential impact that unauthorized disclosure or access will have on the security posture of the component in question.
- **Lack of Availability**: The student should consider the implications that lack of water would have on the hospitals in the region. What would happen if an adversary dumped toxins into primary river confluences? What are the impacts on industry and the economy if lack of availability lasted more than 48 hours?
- **Loss or Destruction**: This can have an extreme psychological impact on users who depend on our critical infrastructures. Suppose the salinity provision numbers were changed or deleted and fish died or

people with low sodium tolerance consumed water with inordinate levels of salt? Supposed the filtering plant caught fire? These questions must be considered in identification of critical infrastructure security requirements.

C. THREAT AND VULNERABILITY ANALYSIS

The third phase of CIP strategy framework development is a threat and vulnerability analysis. In this step, the student is interpreting, summarizing, and predicting. Alberts and Dorofee (2003) advocate development of a generic threat profile. This threat profile is a catalog of threats that lists all potentially viable threats. This includes assessing the amount of sensitive information available to the public, access to the asset and the potential outcome of that asset being compromised. One tool for doing this in the classroom is the use of attack trees. For more information see Alberts and Dorofee (2003).

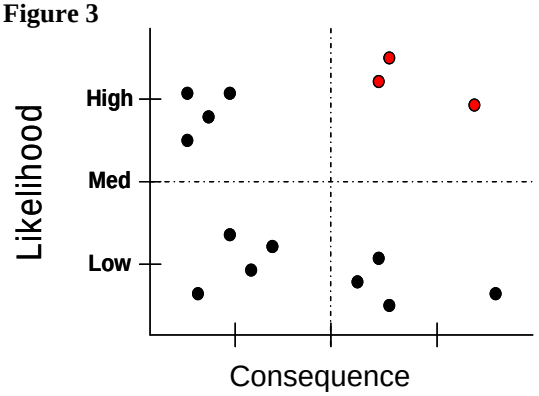
The student should perform a threat analysis that contains three basic steps: (1) list; (2) group; and (3) characterize. The student should list all possible and viable threats to the SRB. Next, the student should characterize these threats by impact theme. For example, the theme could be economic, industrial, fear, or loss of life. Once the threats are organized into themes, the student should be able to identify redundancies and prioritize the threats by likelihood. The point is that the student should have the opportunity to predict and provide rationale for predictions. Establishing a viable set of threats from multiple perspectives (levels of management) will produce a robust risk assessment (to be discussed later).

Once the threat analysis is complete, the students should complete a work plan for performing a vulnerability analysis. This plan should contain the judicious (when? why? how?) use of scanning tools, network mappers, password crackers, and operating system security posture assessments. Once the threat and vulnerability analysis is complete, the students can move on to the risk analysis phase.

D. RISK ANALYSIS

During this step, the student is also interpreting, summarizing, and predicting. Quantifying risk is the biggest challenge as there will be dissenting opinions on what a 0.75 probability and a .82 probability of attack really mean. For instructional purposes, students should start with a simple high-level risk assessment. Specifically, using the SRB scenario described earlier, define three categories—high, medium, and low—for both likelihood and consequence, and map the threats to the grid shown in Figure 3 below.

Figure 3



The dots in the upper right quadrant represent those threats that have the highest likelihood and the highest consequence. For example, toxic dumping or filtration plant failure could represent two of the three dots in the upper right quadrant. This process is at best imperfect. However, it will give the student a visual characterization of the outcome of the threat and vulnerability components discussed above and lay the foundation for developing a CIP strategy framework.

VII. DEVELOPING AND EXECUTING A CIP STRATEGY FRAMEWORK

Now that the student understands the issues that a CIP strategy addresses, how do we create one? A CIP strategy defines the initiatives an infrastructure organization uses to enable initiate, implement, and maintain its security posture (Alberts & Dorofee, 2003). This strategy framework should include, where appropriate, enforcement mechanisms. The Risk Assessment described above is the primary driver of the CIP strategy framework. This phase provides opportunities for the students to apply what they know, analyze what they applied, synthesize the analysis into different contexts, and evaluate the results. The strategy framework, at a minimum should include the following components:

- **Disaster Recovery/Contingency planning**: What should be done if the SRB experiences a major interruption? Are backup resources working and available. The student should be able to develop high-level contingency plans that can be used in any CI component. Moreover, the students should provide strategies for making sure employees at all levels are cognizant of the plan. The student should be able to develop a Disaster recovery strategy for multiple CI components, identify similarities and differences and explain the rationale behind these similarities and differences. Very few CI components have Disaster Recovery plans and procedures in place. If they do exist, they are often out of date.

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

- **Information Security Policy**: At a minimum, data and network protection strategies are imperative because data enables the CI components. The student should be able to make judicious decisions about technology use for convenience vice secure use of technology. Users sharing passwords or who fail to create good passwords should be denied access until they comply with infrastructure security rules and regulations. In short, the security rules of engagement should be well-defined in an operational environment like electrical power delivery.

  In different situations, either policy will drive requirements or requirements will drive policy. The student should understand the impact of each situation. Students should develop an information protection policy for a critical infrastructure component. The security policy should be reassessed every year. The CIP strategy should adapt to the infrastructure component in question.

- **Operations Security (OPSEC):** The goal of OPSEC is to control information and observable actions about your capabilities and intentions in order to keep them from being used by your adversary. OPSEC is a process that teaches you: (1) to examine your day-to-day activities from an adversary's point of view; (2) to understand what an adversary can learn about you and/or your organization from these activities (observables); (3) to assess the amount of risk this places on you and/or your organization; and (4) to develop and apply countermeasures so that the bad guys don't win[18]. Using the SRB scenario described earlier as an example, the first step should be to make the map more generic and provide detailed information to those who have a need-to-know.

- **Risk Mitigation**: The students should explore ways to mitigate risk. This means quantifying the costs of the dots in the upper right-hand quadrant of Figure 3 discussed earlier and presenting this case to senior management.

- **Security Architecture**: Is there a security architecture for the SRB? The risk assessment will provide insight into security architecture development. The student must understand that the security architecture is a roadmap and may be the same in every infrastructure. The way the architecture is implemented will be the only differentiator!

- **Security Awareness and Training**: This component is usually saved for after the fact. In most cases, security training and awareness is often seen as the new initiative levied on the workforce by management. Students should develop and brainstorm about security awareness and training strategies that is stakeholder driven. Conducting periodic security awareness exercises is the best way to maintain a strong Critical Infrastructure security posture.

VIII. CONCLUSION

This paper makes the case for educators and curriculum developers to broaden current Information Assurance – focused curriculum, concepts and pedagogies to include" Infrastructure Assurance." This paper discussed the notion of convergence theory--the next attack will be a blended attack of physical and cyber dimensions; (2) identified CI components that comprise the U.S Critical Infrastructure;(3) discussed the notion of "Infrastructure Assurance" and its role in current Information Assurance curriculum; and (4) using a regional water supply system scenario, provided a strategy framework for developing a Critical Infrastructure Protection (CIP) strategy and pedagogically integrating Infrastructure Assurance into existing Information Assurance curriculum. This paper provides a framework that can be used as a foundation for broadening existing Information Assurance curriculum. As colleges and universities seek to establish CyberDefense exercises, they should consider the payoff that a CI spin would have on network defense strategies and student learning. Infrastructure Assurance is a tradeoff where you are balancing the need to connect with the need to protect where Geography is History!

IX. REFERENCES

[1] *National Strategy to Secure Cyber Space*. February 12, 2003.
[2] US General Accounting Office, Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors, February 2003.
[3] Moteff, John, Copeland, Claudia, and Fischer, John. "Critical Infrastructures: What Makes an Infrastructure Critical?" Report for Congress. Order Code RL31556: CRS-1.
[4] Lawson, S. M, Information Warfare: An Analysis of the Threat of Cyber Terrorism Towards the US Critical Infrastructure. SANS GSEC, Version 1.2F.
[5] Schepens, W.J., Ragsdale, D. J., and Surdu, J.R. "The Cyber Defense Exercise: An Evaluation of the Effectiveness of Information Assurance Education." *The Journal of Information Security*, Vol 1, Num 2, July 2002.
[6] US General Accounting Office, Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors, February 2003.
[7] Creating a Trusted Information Network for Homeland Security, Second Report of the Markle Foundation Task Force, December 2003.
[8] Crowley, Edward, *Information System Security Curricula Development*, CITC4 '03, October 16-18, 2003, Lafayette, IN.
[9] "Administrative Oversight: Are we ready for a CyberTerror Attack?" Testimony before the Senate Committee on the Judiciary, Subcommittee on

Administrative Oversight and the Courts, by Richard A. Clarke, Special Advisor to the President for Cyberspace Security and Chairman of the President's Critical Infrastructure Protection Board (Feb. 13, 2002).

[10] Verton, Dan. "*Web sites seen as terrorist aids*." Computerworld. 2/11/2002. URL: http://www.computerworld.com/industrytopics/energy/story/0,10801,68181,00.html (August 22, 2003).

[11] "Maps of Nuclear Power Reactors: World Map." International Nuclear Safety Center. URL: http://www.insc.anl.gov/pwrmaps/ (August 15, 2003).

[12] "California Energy Maps." Map of Power Plants in California. June 26, 2003. URL: http://www.energy.ca.gov/maps/power_plant.html (July 8, 2003).

[13] "California Energy Maps." California's Major Electric Transmission Lines. September 6, 2000. URL:http://www.energy.ca.gov/maps/transmission_lines.html (July 8, 2003).

[14] Blumenfeld, Laura. "Dissertation Could Be Security Threat." Washington Post. July 8, 2003. URL: http://www.washingtonpost.com/ac2/wp-dyn/A23689-2003Jul7?language=printer (July 31, 2003).

[15] Adapted from: Bloom, B.S. (Ed.) (1956) Taxonomy of educational objectives: The classification of educational goals: Handbook I, cognitive domain. New York; Toronto: Longmans, Green.

[16] Nutrient and Sediment Loads for SRBC, http://www.srbc.net/guardian/Spring%202004/Page%206%20-%20NutrientandSedimentLoadsDecreasing.pdf.

[17] Alberts, C. and Dorofee, A. (2003) Managing Information Security Risks: The OCTAVE[SM] Approach

[18] What the Heck is OPSEC? http://www.opsec.org/who/who02.htm