Proceedings of the 11th Colloquium for Information Systems Security Education
Boston University
Boston, MA June 4-7, 2007

Assurance Education: The Way ahead in a Network-Centric Environment

W. Vic Maconachy, Department of Defense, Corey D. Schou, Idaho State University

Abstract – This paper discusses aspects of a Network-Centric environment that should be considered as part of an information assurance course for the future.

Index terms – Information Assurance, Information Warfare, Net Centric Environment

I. Introduction

In an address to the nation from the Oval Office, President Bush, remembering the tragic attack on the Twin towers in New York, noted:

> They know that given a choice, people will choose freedom over their extremist ideology. Therefore, their answer is to deny people this choice by raging against the forces of freedom and modernization. This struggle has been called a clash of civilizations. In truth, it is a struggle for civilization. We are fighting to maintain the way of life enjoyed by free nations.[1]

Thus, on the fifth anniversary of tragedy of September 11, 2001, we were reminded of our vulnerability to extremists and we are given a challenge to continue to rise to the occasion and meet that challenge head-on.

The implications for the future of Information Assurance education are enormous. Indeed, we are at a crossroads in our evolution as a discipline. As our nation has evolved into a network centric environment, those who will shoulder the responsibility of protecting our networks will require an increasingly complex understanding of the context in which those networks operate. No longer can we treat the networks as purely technical environments. The networks have evolved as an extension of our society; a microcosm of our beliefs, our values, and our way of life. The networks are integral to the precious freedoms we enjoy and have depended upon.

> This is netcentricity - the power of digital networks to distribute information instantly and without borders. Characterized by global connectivity, real-time collaboration, and rapid and continuous information exchange, netcentricity is a ubiquitous force reshaping every facet of our markets, organizational cultures, and personal lives at the dawn of the twenty-first century.[2]

This increasing connectivity and expanding global collaboration opens new dimensions for Information Assurance professionals, and for the academic institutions producing them. This paper outlines a set of seven challenges for academia to consider in enhancing the current state of Information Assurance higher education.

II. Situational Awareness

Information Assurance professionals will increasingly be called upon to practice their tradecraft while being mindful of constantly changing political, economic, and social forces, -- a continuously adapting information ecosystem. Some of these global forces, as suggested by the President, will be ideological challenges.

> Given the turbulence associated with globalization and rapid change, coupled with the United States' position as the dominant superpower, discomfort with and backlashes against the dominant 'US" economic-social development model are likely to persist and, perhaps, intensify... the backlashes may unfold as part of a more comprehensive disdain for the United States as the hegemonic global state with a deep reservoir of economic, military, technological, and cultural power.[3]

In dealing with global partners, U. S. Information Assurance professionals will require increased understanding and sensitivity to this emergent reaction. Part of this backlash will be increased overt and covert attempts to exploit U. S. information systems. A recent (Dec. 16, 2006) example of this is the exploitation of a Symantec Remote Management Stack Buffer Overflow Vulnerability (CVE-2006-2630)[4] against nine Department of Defense (DoD) hosts by an IP address registered in China.

Theses attacks are not limited to government systems. The era of information warfare has been launched – No more speculation; No more conjecture; No more time to waste. The planet is engaged in the new form of global

exploitation. Information Assurance professional will increasingly be required to stay "in tune" and aware of the total operational context of the networks they defend.

III. The Broader Context of Information Assurance

Information Assurance has emerged as a vital part of our national and regional government and business programs. Information Assurance is now an integral component of corporate operations. Information Assurance is a component of the spectrum of information operations. It is within this broader context that the Information Assurance professional will be operating. Will this require unilateral knowledge and skill development to understand and deal with the cyber aspects of global turbidity? To answer this question one must examine the concept of information operations.

The term information operations, found mostly in Department of Defense (DoD) literature, has yet to emerge with a commonly accepted definition. At one end a Joint Publication # 3-13 defines Information Operations as, "actions taken to affect an adversary's information and information systems, while defending one's own information and information systems."[5] However, as Seward points out, "The actions described in this DoD definition are quite limited in scope. They are tied directly to our own and others' information elements or the systems that pass those elements. Such a definition does not address the cognitive process of human thought, decisions, and actions but is instead oriented at the systems that pass information and the information itself."[6] In an era of information operations, the technology is not the heart of network-centric operation, rather, human and organizational behavior is. While technology enhances our capabilities, it does not define them.[7]

Information Assurance, operating within the context of Information Operations requires varying degrees of understanding of the human components of the networks. I contend that in the future, academia will be required to prepare Information Assurance professionals for work at three levels of operation; (1) Strategic, (2) Operational, and (3) Tactical. All three levels will require varying degrees of knowledge and ability in the net-centricity domain. First, one must examine the context in which net-centricity is emerging. We are standing in the middle of a great moment in history, a time of cultural transition. This transition is much more dramatic than our move from agriculture to industry-based societies. We are in the *Third Wave*, as Toffler chooses to describe it[8]. Toffler and other speak to the awareness that this "wave" brings with it great social changes. Indeed, some theorists predict bloody consequences of cultures in collision as the digital revolution gathers force. It is a decided power shift and that power increasingly emanates from and within the networks.

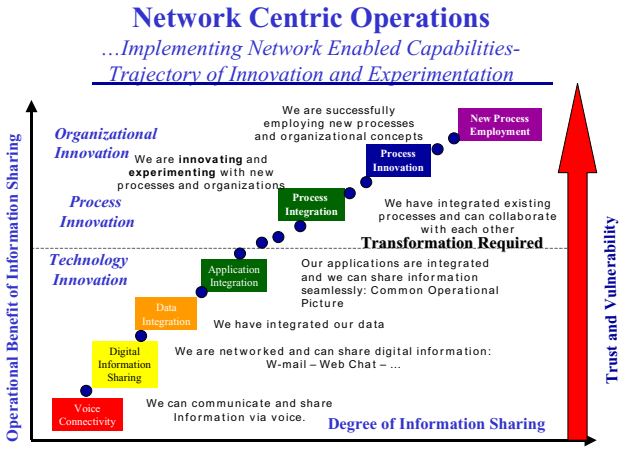

Figure 1 Network-Centric Operations

Figure 1 shows a CIO's dream: Technology as a driver of corporate innovation. Indeed, this sort of graphic is often used to justify increased investment in technology, and new corporate structuring around those capabilities. In fact, as one moves up the chain of technological integration, one shifts into what is called NETWORK-CENTRIC OPERATIONS. Network-centric operations are characterized by Admiral Cebrowski in his 1998 classic, as "information-intensive interactions between computational nodes on the network."[9] "Whether these actions are focused on commerce, education or military operations, there is 'value' that is derived from the content, quality, and timeliness of the information moving between the nodes on the network."[10]

This value of net-centricity increases as information moves towards 100% relevant content, 100% accuracy, and zero time delay – toward something called information superiority. Keep in mind that net-centric operations is a means NOT an objective. It is a tool, NOT a strategy. Net-centric operations are about empowerment.

A. Value, Power, Vulnerability

This thinking about the value which networking brings to any organization is based on the assumption that as the number of information interactions increase, the potential value to the corporation also increases. That might be true in a perfect world. I believe that the potential for a network to create value is a function of the type of information interactions enabled by the network and the value creation logic being employed by the users of the network. Attaining information superiority be it for good or for harm, is not just a matter of increased bandwidth for the sake of bandwidth.

Establishing a direct relationship between information and value is at the heart of value creation in the information age and is fundamental to understanding the power of

network-centric operations. In effect, "dominant competitors across a broad range of areas have made the shift to network-centric operations – and have translated information superiority into significant competitive advantage."[11]

While being a CEOs dream, figure 1 is an Information Security Officer's dilemma. As connectivity and information sharing increase, so do vulnerability and the need for added trust. In the end, cyber security in a networked world is all about one thing: TRUST:

- Trust in the technology
- Trust in the operations and policies
- Trust in the people.

On one hand, information technology and the "networks" they enable play a fundamental role in establishing and defining the network-centric enterprise. Consequently, understanding the underlying trends that govern technology and influence the value-creation potential of networks is important to understanding the power of network-centric-operations. One of the most important trends to consider is the level of vulnerability, created by the increased networking capability, measured against the value of the information being created stored and transmitted on that network.

The increased degree of network centricity requires a greater understanding of those who would do harm to your systems. A first step towards this will be reaching a common understanding of the adversaries' skill levels[12]. Figure 2 illustrates one approach to defining those levels across seven attributes. Adopting this identification model will be a needed first step in reaching a universal classification schema for understanding and discussing cyber adversary level of sophistication and threat. Applying this model would begin with accessing insider threat. This is further developed in a discussion on modeling the insider threat in the Software Engineering institute Technical report on IT Sabotage and Espionage.[13]

ATTRIBUTES	LEVEL 1	LEVEL 2`	LEVEL 3
Level	Inexperienced	Higher order skills	Very sophisticated trade craft
Financing	Limited funding	Well funded	Very well funded
Targeting	Opportunistic	Targeting opportunity	Target technology as well as information
Use of vulnerabilities	Target known vulnerabilities	Target known vulnerabilities	Use unpublished vulnerabilities.
Tools	Use viruses, worms, rudimentary trojans, bots	Use viruses, worms, trojans, bots as means to introduce more sophisticated tools	Use wide range of tradecraft.
Motivation	Is in it for thrills and bragging rights	Target and exploit valuable data	Establish covert presence on sensitive networks
Detectibility	Easily detected	Detectable but hard to attribute	Use of unmitigated code anomaly

Figure 2 Adversary Skill Level

Adopting this or a similar taxonomy allows risk analysts to develop response mechanisms and investments at least equal to the level of threat. This need for reaching common ground in describing degrees of cyber threat is not limited to the protection of just government systems. As a 2006 Department of Defense Report to Congress[14] noted, "China also continues to acquire key technologies and manufacturing methods independent of formal contracts. Industrial espionage in foreign research and production facilities and illegal transfers of technology are used to gain desired capabilities"

A net-centric approach to understanding Information Assurance implies two things. First, we must prepare Information Assurance professionals who can respond technically to the three levels of skill. Second, we should begin adding the components, precepts, and principles of information operations into curriculum. This new curriculum should be oriented toward producing Information Assurance professionals capable of operating in the strategic, operational, and tactical domains.

In this curriculum model, Information Assurance professionals operating at the strategic level need to maintain currency in understanding and forming responses related to the geo political and cultural dimensions posed in a globally connected information infrastructure. The Information Assurance professional working at the operational level must be capable of designing and implementing safeguards in consonance with policies developed at the strategic level. Those safeguards must account for the need to co-exist in a sometimes-hostile cyber space. A broad understanding of the threat base is implicit in being successful at this level. At the tactical level, Information Assurance professionals must apply the safeguards as designed in the operational level. Increasingly, those safeguards will not be limited to just the technical dimension. At the operational level, the Information Assurance professional will be working in a global environment – integrating differing cultures into one team. Customer response units may be located and operated in one nation while customer technical service centers may be responding from another part of the globe. Unless sensitized to geo-political and cultural differences this is the very tipping point for the possible clash of civilizations.

B. Assured Information Sharing

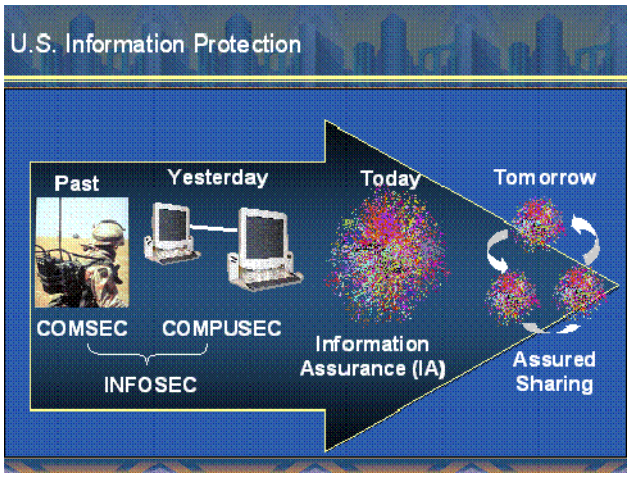

Figure 3 The Emergence of Information Sharing

The priority driving information operations, be it national, regional, or industry-based, will place a greater emphasis information sharing and access as opposed to the current information denial mode. Assured information sharing among partners and clients will become the norm. Figure 3 shows the evolution in thinking leading us to a state of assured information sharing. This transformation will expand our concept of trusted systems to include trusted shareholders and users of our information and our technology. All of this sharing must be viewed in terms of time and ever-changing geo-political and social context.[15] Nowhere could the challenges of assured information sharing be more profound than in the new *Program for Information Sharing Environment* of the Office of the Director of national Intelligence. Figure 4 depicts the cross-domain information sharing requirements between and among communities of interest at varying levels of government and public sector. The plan responds to a national/global need to share terrorism information.

Strengthening our nation's ability to share information Constitutes a cornerstone of our national strategy to protect American people and our institutions and to defeat terrorists and their support networks at home and abroad. Recognizing the need to go beyond individual solutions to create an environment-the aggregation of legal, policy, cultural, organizational and technological conditions-for improving information sharing.[16]

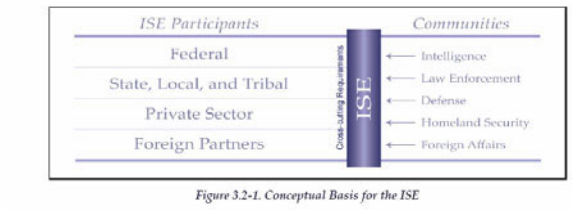

Figure 3.2-1. Conceptual Basis for the ISE

Figure 4 conceptual basis for Information Security Education[17]

As one can see from such a venture, the number of considerations for achieving assured information sharing are enormous. This is the emerging environment of Information Assurance in the near future. Assured information sharing has been one of the "grand challenges of Information Assurance for a decade. It applies at the national level (as above), at the local level (as with fire and police), and in the corporate world of flattened global enterprises. Information Assurance professionals charged with implementing assured information sharing must be global thinkers and conceptual tinkers.

IV. Structured Thinking

The closest academia comes to incorporating a more global view of operating is in the implementation of the Committee for National Security Systems Instruction on Risk Management.[18] Figure 5 (from CNSSI 4016) shows the basic knowledge set required to conduct entry and intermediate level risk management. At the advanced level, the cyber risk analyst is expected to, "Create new solutions to unexpected problems and to interact with and explain cost/benefit to organizational management."[19]

We are in a new era of cyber operations calling for increased risk analysis and management:

- Risk analysis of the technology
- Risk analysis of the operations
- Risk analysis of the people

…all leading to RISK MITIGATION for the systems owners.

The implication for academia is the emergent need to build risk analysis and risk management into all cyber-related courses and programs.

What does this mean for corporations and governments? How will organizations be prepared for this era of trusted and assured information sharing? Our network ecosystems are increasingly at risk –figure 6). In this new era, the information systems security team will no longer be just the technology geeks. They will emerge as a critical corporate asset in understanding BOTH the value of the information to be protected as well as the techniques/costs of protections. They are becoming more and more a trusted agent of the corporate enterprise and critical to mission success. The corporate view of risk management will now include risk as it relates to corporate networks. Return on Investment strategies will be redefined beyond just the bottom line. Sustaining networks, which are trusted by the client base, will be paramount to maintaining corporate information dominance in an increasing cyber context.

Literacy Necessary for a Risk Analyst at the Entry and Intermediate Level	
Access authorization/permission	Hackers and unauthorized users
Accountability	Information Assurance
Assurance	Information integrity
Audit collection	Intrusion
Automated security tools	Integrity
Business recovery	Life cycle system security
Certification & Accreditation	Penetration testing
Change control policies	Personnel security policies
Classification policies	Physical security
Computer crime	Risk analysis
Configuration management	Risk analysis processes
Continuity of operations	Risk management
Cost benefit analysis	Security laws and regulations
Critical assets	Security policy
Data access control	Security safeguards
Denial of service	Security test and evaluation (ST&E) procedures
Detection and response	Social Engineering
Due diligence	System protection profile
Effect of countermeasures	Threat/vulnerability analyses
Environmental/natural threats	Unauthorized system access
Evidence collections	Vulnerability analysis tools
FISMA	

Figure 5 Literacy Requirements for Risk Analysts

In an era when hundreds of new cyber threats are introduced each day into the networks[20] the preparation and maintenance of risk-based cyber defenders is critical to national and corporate cyber survival. The challenge for academia is in equipping future Information Assurance professionals with tools, methodologies, and strategies for keeping pace with the velocity of this assault. Being postured to prepare a resilient Information Assurance work force requires industry, government, and academia to step up research efforts.

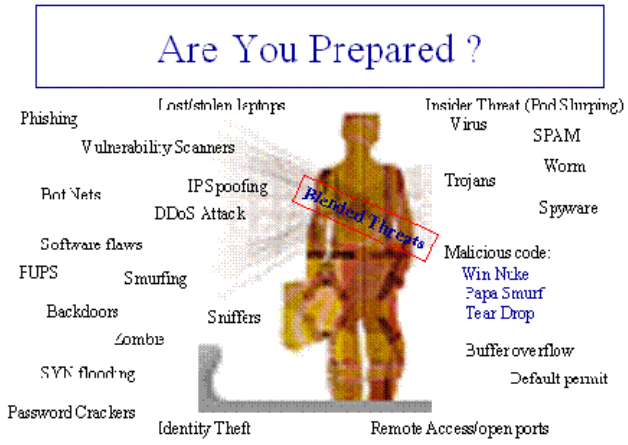

Figure 6 The Era of Blended Threats

V. Changes in our Investment Strategy

In 1928, the British geneticist J.B.S. Haldane wrote a now famous essay entitled, *On Being the Right Size*, where he noted, "The most obvious differences between different animals are differences of size … it is easy to show that a hare could not be as large as a hippopotamus, or a whale as small as a herring. For every type of animal, there is a most convenient size, and a large change in size inevitably carries with it a change of form." It was a cogent argument about surface area to volume ratios, structures, respiration, and energy.

Similar arguments can be made for right-sizing research project resources to challenges and opportunities. The continuum of research opportunities in computing is deep and broad, yet we have often tended to focus on those best attacked by small teams and local infrastructure. Many other disciplines, most notably physics, regularly pursue projects much larger than those common in computing. Such projects often require both substantial intellectual resources (faculty, staff, and students) and major infrastructure investments.

Those projects address fundamental, large-scale problems—sometimes nothing less than the very nature of the universe—and they require multi-institutional teams willing to take risks. I believe we can learn from our peers in the physical sciences: that to address our most fundamental issues and have broad, transforming impact we must "right-size" our research investment portfolio. Developments in areas related to the cyber realm now take on new importance. As areas such as nanotechnology, optics, and quantum computing gain momentum, cyber researchers will be challenged to keep pace. Breakthroughs in those and other areas will have profound influence on the state of cyber space. Those profound influences have, in turn, serious consequences for information assurance. This means balancing risk, from projects with smaller, though highly likely returns on investment, to those that could have a transformative effect, but involve higher risk. This greater diversity in research investment was hinted at in the Federal Plan for Cyber Security and Information Assurance Research Development.[21]:

> The Federal cyber security and information assurance R&D portfolio should support fundamental R&D exploring inherently more secure next-generation technologies that will replace today's patching of the current insecure IT infrastructure.

VI. Summary

As we look back on progress made in establishing information assurance curricula, we cannot rest on our success. Looking ahead to fulfilling the emerging needs of government and industry requires some shifting and expanding of our current approach to preparing Information Assurance professionals. These changes include:

1. Increasing our understanding of all aspects of net-centricity.
2. Preparing students to recognize and be continually aware of their cyber ecosystems.
3. Expanding the gestalt of Information Assurance to enfold Information Assurance into the broader umbrella of information operations.
4. Establishing a common understanding and nomenclature for adversarial capabilities.
5. Stepping up to the challenges of assured information sharing.
6. Increasing our emphasis on risk management/analysis approach to Information Assurance.
7. Changing government and industry investment strategies in Information Assurance research to engage academia in an interdisciplinary fashion.

This call for changes comes at a time of great concern to our nation. A plan for beginning this implementation was developed at a recent Information Warfare conference[22]. Ambassador John Negroponte, perhaps, best summed up the magnitude of the challenge we are facing:

> The issue is America's competitiveness in the fields of science and technology, which was assessed from an economic perspective earlier this year, in an excellent report by the national Academies of Sciences and Engineering and the Institute of medicine. That report called *Rising Above the Gathering Storm* described a world that is being transformed from a scientific and technological perspective at a breath-taking rate of change.[23]

Given this era of rapid transformation the challenge for academia is to continue producing skilled Information Assurance professionals, but also to instill in that work force the broader attributes of resilience and global thinking. We must now think and operate in terms of cyber ecosystems.

VII. References

[1] President George Bush. The White House. September 11, 2006

[2] Robert H. Smith School of Business. University of Maryland. http://www.rhsmith.umd.edu

[3] Central Intelligence Agency. Thinking Ahead. Future Ideological Challenges to US Global leadership. OII TAS 2006-002. November 2006.

[4] http://nvd.nist.gov/nvd.cfm?cvename=CVE-2006-2630

[5] Henry H. Shelton, Joint Pub 3-13: Joint Doctrine for Information Operations. Washington, D.C. U.S. government Printing Office) October 1998.

[6] Andrew B. Seward. U.S. Strategic Information Operations: The requirement for a Common Definition and Organizational Structure In Support of The Global War on Terrorism. U. S. Army War College. Carlisle Barracks, Pennsylvania. Defense Technical Information Center Accession Number ADA424404. May 2004. p 4

[7] David S. Alberts, John J. Garsika, and Frederick P. Stein, Network Centric Warfare: Developing and Leveraging Information Superiority. 2nd ed (rev). Washington, D.C. C4ISR Cooperative Research Program Publications Series August 1998, p 88.

[8] *The Third Wave.* Alvin Toffler. March 1980. Dell Publishing, New York. ISBN: 0553246984

[9] Cebrowski, Arthur K. *Network-Centric Warfare: Its Origin and Future*. U. S. Naval Proceedings, January, 1998.

[10] Technology and the Electronic Company. IEEE Spectrum, Feb., 1997.

[11] Cebrowski, ibid

[12] Maconachy, W.V. , Schou, C. D, Frost, J., and Springer,J. Building an Educational Response to Terrorism: A Multifaceted Problem, A Multidimensional Response, *Information Systems Control Journal*, Volume 6, 2004.

[13] Band, Stephan, Cappelli, Dawn, Fischer, Lynn, Moore, Andrew, Shaw, Eric, and Trzeciak, Randall. Comparing insider IT Sabotage and Espionage: A Model-Based Analysis. *Technical Report # CMU/SEI-2006-TR-026*. CERT. Pittsburgh, PA. December, 2006

[14] U.S. Department of Defense. Annual Report to Congress: Military Power of the Peoples Republic of China, 2006. Office of the Secretary of Defense. Washington, D.C.. November, 2006.

[15] Maconachy, V., Schou, C. Ragsdale, D, & Welch, D A Model for Information Assurance: An integrated Approach. Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, NY, 5-6 June 2001. p 309.

[16] Office of Director of National Intelligence. Information Sharing Environment Implementation Plan. Washington, D.C.. November, 2006.

[17] http://www.oft.osd.mil/library/library_files/briefing_337_Fighting_the_Networked_Force_22_Jan_04_Optimized%20.ppt.

[18] Committee for National Security Systems. CNSSI 4016. National Training and ducation Standard for Risk Management, Washington, D. C. Nov. 2005.

[19] Ibis. P A-3

[20] Computerworld Australia. Quoting *the 2007 Sophos Internet Threat Report*. Australia, Jan. 29, 2007

[21] National Science and Technology Council. Federal Plan for Cyber Security and Information Assurance Research and Development. Arlington, VA. April 2006 p 24.

[22] Corey D. Schou, Kuehl, Armistead: Information Operations Education: Lessons Learned from Information Assurance. Proceedings 4th European Conference on Information Warfare and Security 325-334, University of Glamorgan, UK, 11-12 July 2005

[23] John Negroponte. Remarks of the Director of National Intelligence. Woodrow Wilson International Center for Scholars. Washington, D.C. September 25, 2006