TITLE OF PANEL: Teaching Information Warfare -- Lessons Learned

PANEL CHAIR: Prof.Lance J. Hoffman, The George Washington University

PANELISTS:
1. Prof. Dorothy E. Denning, Georgetown University
2. Dr. Roger Molander, RAND Corporation
3. Prof. Daniel Kuehl, National Defense University

SESSION ABSTRACT

The growing importance of information assurance is reflected in new relevant course offerings at universities, which often include simulations of information warfare scenarios. This panel presents individual descriptions of successes and failures in bringing this topic to the classroom, and touches on where these courses fit in the overall university curricula.

PANELIST STATEMENTS:

Teaching Information Warfare at The George Washington University

Lance J. Hoffman
Computer Science Department
The George Washington University
Washington, DC 20052
hoffman@seas.gwu.edu

Teaching information warfare to a multidisciplinary class with professors from computer science, sociology, and psychology is rewarding, but is also a challenge. We use two textbooks. My colleagues (John Markey of the GWU Sociology Department and Jerrold Post of the Political Psychology Program) and I also use a number of guest lecturers who are practitioners or government officials; they are very well received. However, we have found that our course also requires better thought out "incident scenarios", and may require a battle laboratory that can effectively teach students from various disciplines. Ethical and practical issues associated with these are challenges we look forward to addressing.

This course drew on literature and speakers from the fields of criminal justice, computer security, and transnational security--as well as a semester-long Information Warfare simulation--to explore the political and operational implications of Information Warfare. The home page for the course, with much more detail than this presentation, is at http://www.seas.gwu.edu/classes/cs751.

Students were responsible for a response paper, a group project, and a final, and were expected to actively participate in the class. The group project responded to the simulation, and involved students acting in roles as members of various governmental and non-governmental organizations to develop offensive and defensive IW operations.
The final exam was based on both readings and lectures.

The required texts were:

- Campen, Alan D. and Douglas H. Dearth, ed., *Cyberwar 2.0: Myths, Mysteries and Reality* (Fairfax, VA: AFCEA International Press, 1997).
- Denning, Dorothy, *Information Warfare and Security* (Addison-Wesley, 1998).

Supplementary Readings were either found on the World Wide Web or offered on reserve in the library. Topics included

- 21st Century Warfare,
- Simulating Information Warfare,
- Mapping the Critical Iinfrastructure,
- Protecting Critical Infrastructure: Interdiction and an Enforcement Perspective
- Computer Security-Technical Dimension
- Computer Security-Human Dimension
- Open Source Intelligence
- Solar Sunrise": A Case Study
- G8 Senior Experts Group on Transnational Organized Crime
- Diplomacy and Information Terrorism
- Psychological Operations
- Ethics

Teaching Information Warfare at Georgetown University

Dorothy E. Denning
Georgetown University
Washington, DC
denning@cs.georgetown.edu

COSC 511 Information Warfare: Terrorism, Crime, and National Security, is a 3-credit course at Georgetown University. It has no prerequisites and studies the nature of information warfare, including computer crime and information terrorism, as it relates to national, economic, organizational, and personal security. Students gain an understanding of the threats to information resources, including military and economic espionage, communications eavesdropping, computer break-ins, denial-of-service, destruction and modification of data, distortion and fabrication of information, forgery, control and disruption of information flow, electronic bombs, and psyops and perception management. They learn about countermeasures, including authentication, encryption, auditing, monitoring, intrusion detection, and firewalls, and the limitations of those countermeasures. They learn about cyberspace law and law enforcement, information warfare and the military, and intelligence in the information age. Information warfare policy and ethical issues are examined.

The course is mainly conceptual and analytical. Classes consist of presentations (often by an outside expert in the field) and discussions. Students are given weekly reading assignments in preparation for each class. Course evaluation is based on class participation and weekly writing assignments (50%) and a research paper (50%).

The main texts (supplemented with other readings) are

- Dorothy E. Denning, Information Warfare and Security, Addison-Wesley, 1999.
- Alan D. Campen and Douglas H. Dearth, Cyberwar 2.0: Myths, Mysteries and Realities, AFCEA Press, 1998.
- James Adams, The Next World War, Simon & Schuster, 1998.

The course home page is at http://www.cs.georgetown.edu/~denning/cosc511/spring99/
Topics covered included:

- Introduction to Course and Information Warfare
- Concepts and theory of information warfare. Trends.
- Information Warfare in Context
- Open Sources, Psyops and Perception Management
- Insider Threat, Espionage
- Insider Threat. Competitive intelligence. Economic, corporate, and military espionage. Invasions of privacy.
- Intelligence, Fraud, and Sabotage
- Computer Break-ins, Hacking, Masquerading, Cyberplagues
- Secrecy and Authentication
- Monitors, Gatekeepers, Risk Management, Incident Handling
- The IW Threat
- Defensive IW Policy and Programs
- IW Policy and Ethics

Frameworks and End States in the Teaching of the Strategic and Ethical Dimensions of Strategic Information Warfare

Roger C. Molander
Rand Corporation
Washington DC
molander@rand.org

Strategic information warfare (SIW) refers to that realm of information warfare or information operations that is strategic in character (and potentially truly revolutionary). In the SIW context it is almost impossible to efficiently bring individuals up to speed – and facilitate strategy and policy decision-making or ethical debates - without an intellectual framework on which the many dimensions of SIW and related strategic warfare subjects can be arrayed. Its most useful form, such an intellectual framework is likely to be a series of relatively simple steps – a process – that presents issues that to be addressed in a logical architecture and along a logical path in a fashion that facilitates debate and decision-making.

Recognizing that in the still rapidly evolving SIW arena, the concept of a single temporally stable framework is illusory - that a useful construct must be dynamic, capable of responding to changes in both the security and IT environments - an initial formulation of such a framework can be divided into the following distinct steps:

1. Key Dimensions of the SIW Environment. Gain an understanding of the key dimensions of the future SIW "environment," i.e., those dimensions that might be shaped or influenced (presumably in some favorable direction) by effective near-term strategy and policy decision-making or a consensus on ethical considerations.

2. Key Strategy and Policy Issues. Identify those key near-term strategy and policy issues – and ethical issues - germane to the SIW problem.

3. Current State of SIW. Assess the current state of SIW in terms of absolute and relative offensive and defensive SIW capabilities.

4. Alternative SIW "End States." Craft a set of (plausible and potentially desirable) alternative SIW "End-States" – expressed in terms of the above key dimensions of the SIW environment.

5. Alternative Action Plans. Array the key SIW strategy and policy issues – and ethical issues - against each of these alternative End States and conceptualize action plans for moving from the current state of SIW toward one or more of these end states.

With a framework such as that described above in hand, the myriad of issues associated with the SIW problem can be arrayed or positioned in such a fashion that a student can see these issues in the larger and more complete (and complex) context that is essential to the understanding of the SIW problem. Here the "End States" issue is of the essence. For example almost any initiative/idea can be constructively challenged in the following sequence: (1) What is the SIW end state that you believe is both plausible and the most desirable nationally and globally? and (2) How does your proposed initiative/idea achieve progress toward this end state? An SIW framework developed at RAND proved very effective last year in dealing with the Russian UNGA proposal to initiate arms control negotiations on IW-related matters.

The key dimensions of SIW – from the potential vulnerabilities of critical infrastructures; to the problems of warning, attack assessment, and perpetrator identification; to the potential redeeming quality of being "much more humane" than other forms of strategic warfare (since the only intended casualties would be the crippling of information flow, convenience, and comfort) – are well known. Putting these characteristics and larger SIW issues in an ethical context is much more difficult. Addressing searching end state and ethical questions of this character will require careful study of the strategic, political, technological, and ethical dimensions of the SIW problem.

Teaching Information Warfare and Information Operations at National Defense University

Dan Kuehl
National Defense University
Washington, DC
Kuehld@ndu.edu

Cyberspace has already become a battlespace for international and unconventional conflict. Cyber attacks can deliver "mega-bytes" of infectious electrons from afar without the messiness of physical destruction, or they can be used to influence perceptions and wage war via the "wetware." A new national security education program that anticipates potential threats to critical information and the information infrastructure
is needed to address non-traditional threats, attacks, targets, and means of attack. Strategic decision makers will have to know something about: the legal environment, critical information infrastructures, the economic dimension of national security, information warfare/information operations, and diplomacy in the information age. Lessons learned from current courses and programs at the National Defense University will also be presented.

The Information Strategies Concentration Program (ISCP) is the keystone of the National Defense University (NDU) effort to prepare strategic leaders for the national security implications of the information age.

The Information Operations course at NDU examines Information Operations (IO) concepts and describes the need for a partnership between the CIO and the warfighter to achieve an integrated technical, operational and doctrinal environment. The course discusses the necessity to reengineer mission-critical warfighting and cross-functional processes in order to maximize performance and compatibility in conflict and peacetime competition. Initiatives to implement IO concepts in support of national security strategy and joint warfare are considered, with an emphasis on using operation chain analysis (*aka* value chain analysis) to achieve the IT thread of operational architecture. Discussion includes an assessment of challenges for the CIO, and considers the role of non-DoD government agencies in the process.

This course is appropriate for senior leaders in civilian grades GS/GM 13 through 15 and military grades 0-5 through 0-6 who exploit the information component of national and military power. This includes--but is not limited to--federal and military information operators; Chief Information Officers; military and federal personnel who develop and manage information resources; students in Professional Military Education programs (intermediate and senior). The course is conceptual rather than technical, and requires no technical expertise beyond the ability to perform simple word processing operations.

The goal of this course is to improve the student's awareness of the evolving role of Information Operations in the national security process, the integration of the war-fighting and CIO's planning process, and to facilitate student analysis of critical information-related issues, such as infrastructure protection or encryption that are becoming increasingly important elements of the new national security paradigm.

Course topics include Information Operations & the Revolution in Military Affairs; Information Warfare, Operations, and the Joint Force; Information Assurance; CIO-Warfighter Integration and Operation Chain Analysis; Nonlinearity and Information Operations; The Encryption Issue; The Legal Environment; Cyberterrorism; The Media; The Internet as a Strategic Environment; Information Operations and the Interagency Community; Information Operations and the Intelligence Community; Global Perspectives; Exercise: "The Day After…in Cyberspace"; and National Security in the Information Age.

SHORT BIO OF PANEL CHAIR AND SPEAKERS

Professor Lance J. Hoffman
Computer Science Department and Cyberspace Policy Institute
School of Engineering and Applied Science
The George Washington University
(202) 994-4955
hoffman@seas.gwu.edu
http://www.seas.gwu.edu/seas/institutes/cpi/

Professor Lance J. Hoffman is in charge of the computer security graduate program in computer science at The George Washington University. Author or editor of five books and numerous articles on computer security and privacy, he has headed a number of cryptographic policy projects and is Director of the School of Engineering's Cyberspace Policy Institute. His most recent readings book, *Building in Big Brother*, was the first book devoted to the topic of cryptography policy. A Fellow of the Association for Computing Machinery and a senior member of the Institute of Electrical and Electronic Engineers (IEEE), Dr. Hoffman has served as general chairman of the Conference on Computers, Freedom, and Privacy and is a member of the National Advisory Board of the newsletter Privacy and American Business; he also sits on the Advisory Committee of the Center for Democracy and Technology and is GW's representative to the Advisory Committee of the World Wide Web Consortium. His recent research includes a survey of cryptographic products available outside the United States, development of a privacy policy for an electronic payments system, and risk analyses for telemedicine privacy and security. His recent teaching innovations include multidisciplinary courses on electronic commerce and information warfare.

PROF. DOROTHY DENNING
Computer Science Department
Georgetown University
Washington, DC 20057-1232
http://www.cs.georgetown.edu/~denning
202-687-5703, fax 202-687-1835
e-mail: denning@cs.georgetown.edu

Dr. Dorothy E. Denning is professor of Computer Science and professor and member of the advisory board of the Communication, Culture and Technology program at Georgetown University. Her current work encompasses the areas of information warfare and assurance, encryption policy and technology, and the impact of technology on law enforcement and society. Before coming to Georgetown in 1991, she worked at Digital Equipment Corporation, SRI International, and Purdue University. She has served as president of the International Association for Cryptologic Research, chair of the International Cryptography Institute, and chair of the National Research Council Forum on Rights and Responsibilities of Participants in Networked Communities. She is presently a member of the President's Export Council Subcommittee on Encryption Policy. Denning has testified before Congress on encryption policy and authored more than 100 publications. Her most recent book, Information Warfare and Security, was published by Addison Wesley in late 1999. Denning is an ACM Fellow and

recipient of the 1990 Distinguished Lecture in Computer Security Award. She received the A.B. and A.M. degrees in mathematics from the University of Michigan and the Ph.D. degree in computer science from Purdue University.

Professor Daniel T. Kuehl
School of Information Warfare & Strategy
Information Resources Management College
National Defense University
Ft McNair, Washington DC 29319-6000
202-685-2257//202-685-3664 fax
kuehld@ndu.edu

Dr. Kuehl teaches military strategy and national security policy in the School of Information Warfare & Strategy, an element of the Information Resources Management College at National Defense University in Washington, DC. He is the director of the Information Strategies Concentration Program, a specialized curriculum for selected students at the National War College and Industrial College of the Armed Forces, in which he teaches on the law of war, the strategic use of the internet, and information warfare and strategy. His dissertation focused on the Air Force's employment of electronic warfare in the decade after WW II. In his final assignment at the Air Staff he was part of the "Checkmate" planning team that in August 1990 developed the "Instant Thunder" plan for a strategic air campaign against Iraq, after which he served as chief of the Air Staff element that supported the Secretary of the Air Force's landmark Gulf War Air Power Survey (GWAPS). He authored the "Air Campaign" chapter in the DOD's Final Report to Congress on the Persian Gulf War (also known as the "Title V Report"), and was the editor of the GWAPS volume of Gulf War statistics, A Statistical Compendium. Other publications include articles in Air University Review, Civil War History, Air Power History, Journal of Military History, Journal of Strategic Studies, Joint Force Quarterly, Enjeux Atlantiques, and the Pakistan Defense Journal, and he has contributed chapters to Airpower: Theory and Practice (by Cass), The Eagle in the Desert: Looking Back on US Involvement in the Persian Gulf War (by Praeger), Cyberwar: Security, Strategy and Conflict in the Information Age, and its sequel Cyberwar: Myths, Mysteries and Realities (both published by the Armed Forces Communications and Electronics Association). His most recent publications are "Strategic Information Warfare: a Concept", by the Australian National University's Strategic and Defence Studies Centre in Canberra, and "Information IN War or Information Warfare--is the Distinction Meaningful?", published by The Canadian in Fall 1998. His current research focuses on the relationship between the information age and national security, and he is currently writing a book on the early history of electronic warfare.

Dr. Roger C. Molander
The Rand Corporation
Washington, DC
202 296-5000 ext. 5603
fax 202 452-8377
molander@rand.org

Dr. Roger Molander, a senior research scientist at RAND, currently leads the development of RAND's "Day After..." exercise methodology for exploring new types of strategic conflicts. This methodology was originally developed to explore the counter-nuclear proliferation problem and more recently has been applied to cyberspace warfare against critical U.S. infrastructures; the potential impact of various emerging facets of electronic commerce such as e-cash, Internet banking, and Internet gambling on the U.S. and global anti-money laundering strategy, and the international Y2K problem. Dr. Molander was a member of the National Security Council staff at the White House from 1974 through 1981 where his principal area of responsibility was strategic nuclear arms control. Prior to joining the NSC staff he was employed in the U.S. Department of Defense. From 1981 to 1989 he was involved in developing educational materials on nuclear war and other major national policy issues at Ground Zero and the Roosevelt Center for American Policy Studies. He has a PhD in engineering science and nuclear engineering from the University of California at Berkeley.

BACKGROUND OF AUDIENCE WE ARE TRYING TO ATTRACT:

technical and senior and middle management who did not have an information warfare course when they went to college (or afterwards)