InfowarCon

www.misti.com

MIS TRAINING INSTITUTE

The International Leader in Audit & Information Security Training

InfowarCon *2000*

Assurance Strategies and Solutions

Featured Speakers

- **The Honorable Curt Weldon**
  US Congress
- **Martha Stansell-Gamm**
  Chief, Computer Crime and Intellectual Property, Department of Justice
- **John Tritak**
  Director, Critical Infrastructure Assurance Office
- **Richard A. Clarke**
  National Coordinator for Security, Infrastructure Protection and Counter-Terrorism, National Security Council

Produced by
Winn Schwartau and
MIS Training Institute

Conference & Expo
September 12-13, 2000
Washington, D.C.

Optional Workshops
September 11 & 14

iDEFENSE

infowar.com

Welcome to InfowarCon *2000*

Who Should Attend

- Military personnel in Offensive and Defensive IW, and PSYOPS
- Professionals in electronic civil defense, e-commerce and information protection
- Municipal employees
- Intelligence Agents
- Chief Executive Officers
- Chief Technology Officers
- Managing Directors
- Information Security Directors, Managers, and Staff
- MIS Managers and Staff
- Legal Counselors
- Law Enforcement Officers
- Computer Crime Investigators
- Security Consultants
- Network Security Architects
- Network and LAN Administrators
- Systems Analysts and Administrators
- IT Auditors
- Information Systems Managers and Staff
- Academics in the fields of Computer Science or IW/Strategic Studies
- Anyone responsible for enterprise and infrastructure information assurance and operations

Although Y2K turned out to be a non-event, the new millennium has already witnessed business-crippling cyber attacks, show-stopping technical sabotage, and international acts of terrorism. You need only pick up a newspaper or turn on your television to be reminded how dependent we are on our information infrastructures...and how critical it is for government and commerce to protect them.

Battling Back

InfowarCon 2000 delivers the assurance strategies and solutions you need to protect your enterprise from internal and external attack. In two, information-packed days, this critically acclaimed event will bring together military leaders, political forces, academics, and industry top guns from all over the globe who will share their hard-won expertise.

You will benefit from the first-hand knowledge of in-the-trenches infowarriors from such highly regarded organizations as the Department of Justice, Europol, National Defense University, Georgetown University, Centre for Infrastructural Warfare Studies, KMPG LLP, UK Defence Communications Services, Lucent Technology, US Department of Defense, and more.

Tracking Your Conference Experience

InforwarCon 2000 covers the full gamut of IW topics, including the latest hacker tactics, asymmetric threats, PKI, legal industrial espionage, terrorists and organized crime, cyberweapons, information assurance, cyberterrorist behavior, and much more.

And to help you focus on the areas you are most interested in, sessions are organized into eight, targeted tracks:

- **Law Enforcement**
- **Technology for Commerce and Military Defense**
- **Terrorism**
- **Commercial and Government Cooperation**
- **Infowar: The Human Dimension**
- **Social Aspects of Infowar**
- **Making Security and Assurance Work**
- **IW Student Track on Infrastructure Studies**

Optional Workshops and International Networking

You can leverage your travel time and conference investment by taking an optional, pre- and/or post-conference workshop. And, because *InfowarCon* attracts a global audience, you will have invaluable opportunities to network with colleagues from around the world.

InfowarCon 2000 is the premier source of assurance strategies and solutions. We look forward to being your hosts in Washington, DC.

Sincerely,

Michael I. Sobol, CISA
Chairman
MIS Training Institute

Winn Schwartau
Founder, Infowar.Com
CEO, Interpact, Inc.

18 Strategic Reasons to Attend

You will:

- Find out what law enforcement officials need to know to track down and prosecute cybercriminals
- Delve into information operations that can be used to support unconventional warfare, and learn how to counter these activities
- Cover the tools, tactics, and players typically involved in economic espionage and the strategies both the public and private sectors are using to defend against them
- Explore the human factors of information warfare and the dangers of over-estimating the defense value of even the best technologies
- Get the lowdown on what the Defense Advance Research Projects Agency (DARPA) is doing to create a behavioral model of today's cyberterrorist
- Discover how the principles of business marketing campaigns can be applied to information and psychological operations
- Identify the five tenets of information assurance and learn how to use each to ensure the integrity of your data
- Learn how strong crypto and difficult tracking techniques allow terrorists to use the Internet for large-scale criminal activities
- Take a look at asymmetric threats and how they impact the practicalities of IW
- Examine the need for a national security awareness program to educate the public about IW and learn how you can help achieve this initiative
- Hear about the latest initiatives being developed by the Critical Infrastructure Assurance Office (CIAO) to boost national security
- Review China's 36 historical stratagems and their potential application to IW
- Define perception management and the role PSYOPS and deception play in modern conflict
- Learn how organized crime is using high tech and the Internet to carry on illegal activities to fund cyberterrorism
- Benefit from the innovative ideas of some of the best students from top universities and military schools in the unique Infrastructure Studies track
- Walk through a series of scenarios that will let you develop strategies you can use to defend against network attacks
- Determine the reasons why consumer groups are pushing for increased government oversight to protect private information and learn why security does not always equal privacy in the US
- Survey the IO/IW training and education efforts taking place in the US and UK

About MIS Training Institute

Now in its 22nd year, MIS Training Institute is the international leader in information security and audit training. MIS offers over 90 seminars and a variety of products and services that include on-site programs, conferences, and symposia.

About Interpact, Inc.

Interpact, Inc. is a security consulting organization specializing in penetration studies, security systems architecture, strategic gaming and electronic civil defense. www.infowar.com is the premier Web site for information about infowar and infosec.

Special Conference Features

A Faculty of Hands-On Experts

You'll gain proven techniques and broad perspectives from presenters that include in-the-trenches pros from the military, private, and political arenas. These front-line experts have seen it all, done it all, and done it better than anyone else.

Complete Conference Materials

Materials for all sessions (excluding workshops)—whether you attended them or not—will be posted on the Web after the conference. Attendees will receive a code to access the materials, which include case studies, guidelines, comparisons, checklists, and more. You will receive hand-outs for the sessions you attend.

Team Discount

When four people from your organization attend, each will receive a 20% discount. All registrations must be made and paid for at the same time.

"NETOPPS"

Networking opportunities abound at *InfowarCon*. Scheduled receptions, luncheons, refreshment breaks, and impromptu discussions provide ideal backdrops for swapping ideas with colleagues and turning conference speakers into personal "consultants."

Vendor Expo

Leading vendors of security products and services will be on hand to demo their offerings and answer your questions.

In-Depth Workshops

Optional workshops before and after *InfowarCon* let you leverage your travel time and take advantage of intensive learning opportunities.

Continuing Education Credits

Attendees will be eligible to receive 15 CEUs for the conference and 7 for each workshop.

Optional, Full-Day Workshops

Monday September 11, 2000

9:00 AM - 5:00 PM

W1: Legal Issues in Cyberspace and the Use of Force

Gary Sharp, Esq., Author, CyberSpace and the Use of Force

In this revealing workshop you will focus on the offensive and defensive legal challenges surrounding information warfare. You will find out what the warfighter/operator and his or her legal adviser need to know about the peacetime regime, the law of conflict management, and the law of war. You will cover such critical issues as what constitutes a use of force in cyberspace, and what is legal and illegal under the law of armed conflict. You will learn how to use a decision-support tool that is used to assist warfighters and JAG in legal analysis, and perform legal analysis of case studies to reinforce what you have learned.

W2: Countering the Dangerous IT Insider

Jerrold M. Post, M.D., President; Eric D. Shaw, Ph.D., Director, Research, Political Psychology Associates, Ltd.

While hackers continue to grab headlines, a far more serious threat to corporate information systems and critical data is the trusted insider who has the expertise and the position to damage and destroy valuable information assets. In this workshop you will explore the characteristics and motivations of at-risk employees. You will cover perpetrator profiles and case studies, and examine such solutions for mitigating insider threats as pre-employment screening, identification, and monitoring

W3: Everything You Wanted to Know About Global IW but Were Afraid to Ask

Lt. Col. Perry Luzwick, USAF, Department of Defense; Dr. Gerald L. Kovacich, CFE, CPP, CISSP, ShockwaveWriters.Com; Andy Jones, Group Manager, Secure Information Systems, DERA, UK

In this detailed workshop you will look at the need for full-spectrum IW countermeasures in today's global environment, including organizing and staffing for IW; appropriately using soft capabilities such as psychological operations, public affairs, and mis/disinformation; improving security for software and hardware; promoting education and training; and gaining leadership support. You will define IW: what it is, what it is not; who is doing what to whom; and what it means from a business standpoint. You will get the European and Asian perspectives on IW and analyze case studies involving commercial off-the-shelf security concerns and vulnerabilities and e-commerce challenges.

W4: Running a Successful Computer Crime Investigation and Prosecution

Jim Christy, Law Enforcement & Counterintelligence Coordinator, Defense-Wide Information Assurance Program, ASDC3I

In this step-by-step workshop you will go through the full gamut of a computer crime investigation and prosecution, including building a forensics lab, conducting field forensics, and collecting and safeguarding evidence. You will investigate the statutes that apply to computer crime prosecutions, learn which court orders are useful, and discover why damage assessments are critical to your case. You will also get an unbiased look at available computer investigative training programs. You will put everything you have learned to use in a case-study crime scenario.

W5: Hacking 201

Tim Rosenberg, Esq.; Roger Rosenberg Colonel USAF (Ret.); Erik Naylor, Ph.D.; Ed Naylor, Retired Federal Agent; White Wolf Survival, Inc.

In this exciting workshop you will view live demos of the methods hackers use in target reconnaissance and probes launched to gather data.You will learn how they use the gleaned information for attack selection and execution.You will view an attack from both sides: what the attacker does and what the target sees. You will review effective responses, and cover policy, physical and personnel security, and other factors that are needed to prevent, detect, defend against, and respond to an attack. *All participants in this workshop can take part in a 90-minute, hands-on lab scheduled during the two-day conference. Limited to 12 people at a time, the lab will simulate an attack.*

W6: The Essentials of Building ISACs

James Adams, CEO; Andy Meldrum COO; Cathy Summers, CTO; Dan Owen, Vice President for Intelligence; Bob Giovagnoni, Head of Strategic Relations; iDEFENSE

An Information Sharing and Analysis Center (ISAC) is an essential tool for today's business sectors and government to defend themselves against vulnerabilities. Only through an ISAC can each of these entities understand and effectively manage cyberspace threats on a global scale. So, just what should an ISAC look like and how can it be made to work? You'll find out in this strategic workshop as leaders from iDEFENSE walk you through the steps necessary to build ISACs for both the private and public sector. You will learn how to establish, gather, and share intelligence about threats and vulnerabilities in cyberspace, and discover how ISACs can and do work.

Thursday September 14, 2000

9:00 AM - 5:00 PM

W7: Maintaining Real-Time Operational Continuity: The Fusion of Cyber-Defense and Disaster Recovery

Dennis McCallum, Paul Zavidniak, Greg Swain, Members of the Technical Staff, LOGICON, Inc., A Northrup-Grumman Company; Anita D'Amico, Consultant, Applied Visions, Inc.

As our reliance on information systems in all aspects of our lives continues to grow, a delay in a system restart following a cyber attack could very well prove to be fatal. As a result, the focus of disaster recovery and disaster planning is now being fused with recovery from cyber attacks. In this riveting workshop you will explore what is being done to accomplish recovery in real time while maintaining sustained business operations. Looking at the issues from both the military and business perspectives, you will learn how to structure and maintain an effective continuity plan.

W8: Beyond Open Source: The Real Intelligence Revolution

William Church, Managing Director, Centre for Infrastructural Warfare Studies

In this strategic workshop you will learn how to use the Internet to gather detailed intelligence by building Webs of "honeypots" to trap and identify information and personnel that can be targeted for later use. You will find out how to build a "honeypot" structure, capture passwords and identify users. You will cover such techniques as data mining with Data Text Definition (DTD) and XML, turning data into real-time intelligence, running an intelligence organization on the Web, and conducting information operations from a Web of "honeypots".

W9: The ABCs of PKI

Daniel Blum, Consultant, The Burton Group, Inc.; Contributor to Network World

In this workshop you will take a look at what PKI is, what is can do for the enterprise and what you need to deploy one. You will cover the types of available encryption, data concealment, key lengths and key escrows, and you will weigh the pros and cons of public and shared keys. You will drill down to the essentials of PKI, defining the elements that must be in place to successfully implement one.

W10: Spying on Your Competitors: Legal Industrial Espionage

Jamie C. Pole, Principal Consultant, J.C. Pole & Associates, Inc.

Although a significant percentage of the practices used to conduct industrial espionage are illegal, there are many legal and very effective techniques for gathering intelligence on competitors. In this dramatic workshop you will learn what constitutes legal espionage and how to thwart it. You will cover such techniques as gathering competitive intelligence and evaluating the relevance of obtained information, as well as legal methods for substantiating questionable intelligence.

W11: Information Warfare: A Winning Tool for 2000 and Beyond

Professor Fred Levien, (Ret.), Founding Chairman, IW Department, Naval Post Graduate School

In this workshop you will examine the reality of IW and the drivers and enablers behind it. You will look at the technological underpinnings of IW weapons, including computer security; directed energy weapons such as lasers and HPM; and surveillance, navigation and communications satellites. You will explore, cyber attacks that are designed to take down a grid. You will cover the technical, political and legal limitations surrounding this new mode of warfighting, and review the role of IW in the recent war in Kosovo.

W12: Signals vs. Noise: Retrieving Important Information

J.D. Walker, President; Bob Schubring, Vice President, Public Affairs; Citizens Against Police and Prosecutorial Corruption

In this workshop you will hear how a small, dedicated team of experts using commercial and off-the-shelf equipment, recovered meaningful audio and video evidence from magnetic or other media. Looking at enhanced images, you will receive a hands-on tutorial on recovering seemingly lost details. You will also cover audio enhancement, including techniques for defeating white and black noise generators and tools you can use to retrieve whispered conversations from recordings. You will explore digital filtering as a way to identify word patterns and learn techniques for rapid resolution of word pattern identity. You will get tips on recovering signals from noise in real time.

A basic knowledge of MS-DOS or Windows 95 is required. Participants are encouraged to bring imagery with them, in a digital format on diskette, CD-ROM, or 100 MB ZIP disk, in MS-DOS or Windows 95 compatible file format, or on videocassette.

Sessions

Tuesday
September 12, 2000

8:30 AM - 9:00 AM
Keynote Address
What's Hot in Computer Crime in the Department of Justice
Martha Stansell-Gamm, Chief, Computer Crime and Intellectual Property, Department of Justice

In her keynote address, Ms. Stansell-Gamm will provide riveting insights into the current trends in computer crime. In addition, she will reveal what the DOJ is doing to interface with agencies at the federal and local level to catch the perpetrators.

9:00 AM - 9:30 AM
Keynote Address
Privacy Concerns
A high-level official from NSA will address privacy issues.

Plenary Sessions

9:30 AM - 10:00 AM
1: Asymmetric Threats
Commodore Patrick J. Tyrrell, Defence Communications Services Agency, U.K.

Asymmetric threats have existed since one caveman picked up a stone and used it to batter his less innovative opponent. In this session you will examine what makes people act in one way and not another. You will determine what these human traits mean in cyberspace and how they impact the practicalities of information warfare.

10:30 AM - 11:00 AM
2: The Human Factor in Infowar
Ralph Peters, Author

In this session you will look at the human face of IW. You will examine self-correcting vs. directed societies, and the defense and security capabilities of each. You will cover the limits of IW in asymmetrical conflicts; the difficulties traditional military organizations encounter with informational dynamism; the slow-kill of cultural encounters; and the hyper-violence of failing cultures.

11:00 AM - 11:30 AM
3: The Economics of Information Security
Paul Strassmann, Adjunct Professor, School of IW, National Defense University

In this session you will discover how the principles of risk management, as developed by the insurance industry, offer the best economic cost/benefit models for allocating funds for information security. You will learn why insurance practices that dictate the adoption of codes, standards, independent inspection, risk-pooling and reinsurance can also apply to information warfare situations. You will also review examples of extortion, ransom, and arson insurance policies that will illustrate practices that can be used when handling information warfare exposures.

11:30 AM - 12:00 PM
4: Taking It to the People: National Security Awareness
Winn Schwartau, CEO, Interpact, Inc.; Founder, Infowar.Com

Most Americans today do not really understand what infowar and cyberwar are all about, or how it affects their lives. In this intriguing session Winn Schwartau, a recognized pioneer in the field of information warfare, proposes a national security awareness program as a way to educate the public.

12:30 PM
Luncheon Address:
Distributed ACCRUAL of Service (DAOS) Attacks
Rob Rosenberger, Security Consultant

Virus hoax guru Rob Rosenberger is back to apply his particular brand of humor to DAOS attacks. A serious topic in anyone else's hands...but Rob is a pro at making people laugh when they shouldn't.

Concurrent Sessions

1:30 PM - 3:00 PM
5: Law Enforcement's Role in Incident Response
Jim Christy, Law Enforcement & Counterintelligence Coordinator, Defense-Wide Information Assurance Program, ASDC31; Tom Talleur, Managing Director, Cyber and Technology Investigations, Forensics and Litigation Services, KPMG LLP

In this session Jim Christy will tackle the *Role of Law Enforcement in Incident Response*. Then Tom Talleur will turn his attention to *Terrorists, Organized Crime, and the Internet*. You will discover how the proliferation of strong crypto, true anonymity and difficult tracking techniques have provided terrorists and organized crime with the tools to use the Net for criminal activities.

Track: Law Enforcement

1:30 PM - 3:00 PM
6: Cyberweapon Control
Panelists: William Cheswick, Senior Security Researcher, Bell Labs, Lucent Technology; Richard Downing, Computer Crime and Intellectual Property Section, U.S. Department of Justice; Dietrich Neumann, General Secretariat of the Council of the European Union

Explore issues and options relating to possible cyber-weapon controls and a provision in the Council of Europe's draft CyberCrime Convention that would enact such controls.

Track: Technology for Commerce and Military Defense

1:30 PM - 3:00 PM
7: Superterrorism in the 21st Century: WMD and Cyberterrorism
Panelists: Robert E. Stevens, Sr. Technical Manager, Special Projects Dept., ITT Industries and formerly of US State Dept. Detailed to NIPC; Prof. Yonah Alexander, Senior Fellow and Director, International Center for Counter Terrorism Studies, Potomac Institute for Policy Studies; Dr. M. Anthony Fainberg, Chief/Advanced Concepts Division, Advanced Systems & Concepts Office, Defense Threat Reduction Agency, Department of Defense; Milton M. Hoenig, Ph.D., Private Consultant; Dr. Rodney Jones, President, Policy Architects International

The specter of WMD weapons employed in coordination with cyber attacks against civilian populations is the most daunting terrorist scenario of the 21st century. Such strikes could even be viewed as trial runs for an armed attack from a foreign state, and the increasing connections between organized crime and terrorist cells only serve to amplify this threat. In this session you will hear a panel of experts from the government and the private sector exchange ideas and present strategies for dealing with this menace.

Track: Terrorism

1:30 PM - 5:00 PM
8: The New Face of Economic Espionage: Offense and Defense in the Infosphere
Cyber and Physical Security Experts from NSA, ISS, Booze-Allen Hamilton, The Hart Group and iDEFENSE

In this session you will focus on both state-sponsored and corporate-sponsored theft of proprietary information. You will cover the tools, tactics, and players typically involved in economic espionage and the damage it can cause. You will take a look at the growing offensive capabilities of economic espionage, as well as the defensive tactics being used by the public and private sectors.

Track: Commercial and Government Cooperation

1:30 PM - 3:00 PM
9: Introduction to Perception Management for the Warfighter
Moderator: D.H. Dearth, Course Director, JMITC, Author and Lecturer. Panelists: Dr. Michael E. Vlahos, Consultant to John Hopkins Applied Physics Lab; Col. Alan D. Campen, USAF (Ret.), AFCEA

This session will look at enabling warfighters in the conduct of perception management operations to augment their military campaigns. D.H. Dearth will moderate panel discussions by Dr. Michael E. Vlahos on *The Human Target*, and Colonel Alan D. Campen on *Technologies, Values, and Privacy.*

Track: Infowar: The Human Dimension

1:30 PM - 3:00 PM
10: Waging Public Relations
R. Pierce Reid, VP, Schwartz Communications

In this session you will learn how businesses conduct marketing campaigns and then apply every step of the process to its related information/psychological operations equivalent. You will cover market research and audience analysis; message development; media targeting; press relations; branding; launches; guerilla PR; and other steps designed to rally consumers behind a product, service or idea...and discover how to use them in I/O.

Track: Social Aspects on Infowar

3:30 PM - 5:00 PM
11: Practical Law Enforcement vs. Ineffectual Policies
Moderator: Paulo Felix, First Officer, Open Sources & Documentation Unit, Intelligence Analysis Dept., Europol; Panelists: Commander Dave Pettinari, Pueblo County Sheriff's Office; Tom Talleur, Managing Director, Cyber and Technology Investigations, Forensics and Litigation Services, KMPG LLP

This session focuses on the roles law enforcement can play in combating cyber criminals. Tom Talleur will bring his insights to the issue of how much law enforcement can really do to investigate and solve cybercrimes. He will explore the need for a new and wider scope of permissible activities for law enforcement to use. He will look at the problem of coordinating with other countries and their differing laws. Commander Dave Pettinari will examine hacking situations where local police may not be prepared to investigate cyber intrusions.

Track: Law Enforcement

3:30 PM - 5:00 PM
12: Information Assurance: Protecting Information Assets and Establishing Trust in a Networked Society
John Thomas, Col., US Army, (Ret.), Vice President, AverStar Systems Group; former Commander of the Global Network Operations & Security Center of DISA

CEOs, CIOs and IT managers must address their organization's infrastructure and information assurance and security or risk failure in today's Internet economy. In this comprehensive session you will explore the five tenets of information assurance—authentication, integrity, availability, confidentiality, and non-repudiation—and learn how to use each to ensure the safety of your critical information.

Track: Technology for Commerce and Military Defense

3:30 PM - 5:00 PM
13: Operational Security
Richard Forno, Author, The Art of Information Warfare; Jon C. Concheff, CW4, Special Forces Operations (Ret.)

In the first part of this session, Richard Forno will dispel the myth that technical security is all that's needed to keep secrets, and reveal the ways we are our own enemy. He will demonstrate how people disclose information that can potentially aid an adversary. Then, you will cover *Information Operations in Support of Unconventional Warfare* with Jon C. Concheff. You will examine theft, modification, and destruction of information and the information infrastructure, and how these techniques can be executed without detection or attribution. You will discover how viruses can be planted within information systems, timed to coincide with other operations or simply placed into a system with the intention of denying, disrupting or destroying service. You will learn how financial accounts can be attacked electronically.

Track: Making Security and Assurance Work

3:30 PM - 5:00 PM
14: Critical Infrastructures: Human Perspectives
Moderator: Commodore Patrick J. Tyrrell, Royal Navy, Deputy Chief Executive and Operations Director, UK Defence Communications Services Agency; Panelists: Dr. Andrew Rathmell, Deputy Director of Studies, International Centre for Security Analysis, Department of War Studies, King's College London; Dr. Dan Wiener, Former Government Official and Consultant to Unisys Corporation; LTC (Dr.) Mike McNamara, USA, Chair of the Information Operations Department, National Defense University

This panel discussion will give a human dimension to infrastructure protection. You will hear Dr. Andrew Rathmell talk about *International Perspectives in Infrastructure Protection*; Dr. Dan Wiener address *Private Sector Equities in Infrastructure Protection*; and LTC (Dr.) Mike McNamara cover *Insider Profiling*.

Track: Infowar: The Human Dimension

3:30 PM - 5:00 PM

15: How Much Civil Liberty and Privacy Do We Have to Give Up to Gain Cyber Defense?

Moderator: Winn Schwartau, CEO, Interpact, Inc.; Founder, Infowar.Com; Wayne Madsen, EPIC; William Church, Managing Director, Infrastructural Warfare Studies

How much privacy do we have to give up to achieve a reasonable level of national cyber security? In this give-and-take session noted privacy advocates will take on those who feel that strong security is best achieved with strong controls.

Track: Social Aspects of Infowar

Wednesday September 13, 2000

8:30 AM - 9:00 AM

Keynote Address

Infrastructure Protection and National Security: A Legislative Review

The Honorable Curt Weldon, (R), US Congress, 7th District, Pennsylvania

A hit at last year's conference, Congressman Weldon is back to give us a legislative review of how the government has advanced its protection of the infrastructure and cybersecurity. Get the inside scoop on what this nation's lawmakers are doing about conflict in cyberspace.

9:00 AM - 9:30 AM

Keynote Address

Current Initiatives of the CIAO

John Tritak, Director, Critical Infrastructure Assurance Office

The PCCIP was the forerunner to the Critical Infrastructure Assurance Office (CIAO), the first national effort to address the vulnerabilities created in the new information age. CIAO is charged with formulating a national strategy for protecting our critical infrastructures from physical and cyber threats. Mr. Tritak, CIAO Director, will brief us on the steps that are being taken to boost the defense of our national security, including the formulation of CICG.

9:30 AM - 10:00 AM

Keynote Address

Defending America's Cyberspace

Richard A. Clarke, National Coordinator for Security, Infrastructure Protection and Counter-Terrorism, National Security Council

Plenary Sessions

10:30 AM - 11:00 AM

16: Chinese IW 101

Lt. Col. Timothy L. Thomas, US Army, (Ret.), Analyst, US Army Foreign Military Studies Office, Fort Leavenworth; Adjunct Professor at the US Army's Eurasian Institute, Germany

In this session you will cover Chinese IW terminology and concepts, organizational structure, and three significant works in this area, *Deterring IW, Introduction to IW*, and *Unrestricted Warfare*. You will examine Chinese military exercises conducted to date, and explore how they differ from the U.S. and Russian exercises. You will take a brief look at China's 36 historical stratagems and their potential application to IW.

11:00 AM - 11:30 AM

17: Creating Private-Sector National Cybersecurity: Five Necessary Steps

Dave McCurdy, President, Electronics Industry Association

11:30 AM - 12:00 PM

18: The New Information Warfare Paradigm

John Adams, CEO, Infrastructure Defense, Inc.

The nation-state is rapidly becoming an after-thought in the global economy. While the private sector swiftly supercedes the power and authority of the public sector, huge fissures are opening up and being capitalized on by savvy practitioners of information warfare who are creating a new and especially dangerous IW model. In this timely session James Adams, CEO of Infrastructure Defense, Inc., will cover this phenomenon and walk you through the steps the government and corporations are taking to defend themselves against this cyber threat.

Concurrent Sessions

1:30 PM - 3:00 PM

19: Privacy vs. Security: What Is the Government Doing to Help Us?

Mark M. Pollitt, Unit Chief, Federal Bureau of Investigation; Susan Kelley Koeppen, Information Risk Management, KPMG LLP

In this, two-part session Mark Pollitt, will focus on some of the current initiatives that support law enforcement investigations of cyber crime. Then Susan Koeppen will shine the spotlight on the *Privacy vs. Security* controversy. Even though security is an important component of information privacy, network security alone will not protect privacy. In this timely session you will learn why consumer groups are pushing for increased government oversight, and why the federal government and many states are considering legislation. You will also find out why security does not equal privacy.

Track: Law Enforcement

1:30 PM - 3:00 PM

20: Active Defense Technologies

Anita D'Amico, Ph.D., Director, Secure Decisions, a Division of Applied Visions, Inc.; Christopher Berlandier CEO and CTO, and Fred Villela, Executive Director, SecureSoft Systems, Inc.

You will first explore *Cyber Defense Situational Awareness and Visualization* with Anita D'Amico. You will examine the types of information one needs to achieve cyber defense situational awareness, and the tools that are available to facilitate it. Next, Christopher Berlandier and Fred Villela will take you through the *New Dimensions in Security Assurance Management: Using Security Relational Database Technology to Really SECURE the Enterprise.*

Track: Technology for Commerce and Military Defense

1:30 PM - 3:00 PM

21: Modeling the Cyberterrorist's Behavior

Greg Schudel, Sr. Engineer, Information Assurance Program Integration Team, GTE/BBN Technologies; Bradley Wood, Distinguished Member of the Technical Staff, Information Design Assurance Design Team, Sandia National Laboratories

Very little intelligence or solid data exist regarding today's cyberterorists. This session chronicles the efforts of a team at the Defense Advance Research Projects Agency (DARPA) to model and characterize today's cyberterrorist. Find out what DARPA has discovered and get tips for defending against this sophisticated adversary.

Track: Terrorism

1:30 PM - 3:00 PM

22: The Media and Infowar Hype

Michael Zuckerman, Senior Writer, USA Today

In this session you will hold a magnifying glass to the media and learn why its perspective is always going to make the situation appear grimmer than it might actually be. You will hear why it is distracted by pitchmen, uninformed by those who might have a handle on the problem, driven by "ratings" and "circulation" wars, and given to overstating the threat or ignoring the problem.

Track: Social Aspects of Infowar

1:30 PM - 3:00 PM

23: Perception Management for the Warfighter: Soft Weapons

Moderator: D.H. Dearth, Course Director, JMITC, Author and Lecturer; Panelists: Rusty Miller, Senior Fellow at Sytex Inc. and President/CEO of Nemesis Technologies; Colonel Charles A. Williamson, USAF (Ret.), OASD/SOLIC

Emerging IO/IW doctrine recognizes perception management, including PSYOPS, deception, and other mechanisms, as having elevated and integral importance in modern conflict. In this session D.H. Dearth will outline key components of *Perception Management and Soft Weapons*. Rusty Miller will cover *Digital Tradecraft*, and Colonel Charles A. Williamson will address the *Integration of Perception Management Concepts and Capabilities in the Commander's Campaign Plan*.

Track: Infowar: The Human Dimension

1:30 PM - 5:00 PM

24: Infrastructure Studies

Dr. Fred. Levien, (Ret.), Founding Chair, IW Department, Naval Post Graduate School

Dr. Levien will bring us some of the "best of the best" as he assembles military students from top universities and advanced military schools across the nation. These forward thinkers and potential leaders will surprise you with their concepts and vision of what the future holds.

Track: IW Student Track on Infrastructure Studies

3:30 PM - 5:00 PM

25: Organized Crime's Role in IW

Paulo Felix, First Officer, Open Sources & Documentation Unit, Intelligence Analysis Department, Europol; William Church, Managing Director, Centre for Infrastructural Warfare Studies

This two-part session looks at two faces of cyber crime. Paulo Felix will offer a non-classified presentation based on the non-restricted part of a report he presented at the First European Experts Meeting at Europol. He will respond to the question of whether or not we are experiencing new crimes or if criminal organizations are using new technologies to commit traditional crimes and avoid prosecution. Then, William Church will turn his attention to *Organized Crime's Influence on IW*. You will learn how criminal groups have used their Internet skills to conduct espionage and influence public opinion with cyber terrorism tactics.

Track: Law Enforcement

3:30 PM - 5:00 PM

26: Using Deception in Network Defense

William Hutchinson, Associate Head, School of Management Information Systems, Edith Cowan University, Australia

In this session you will go through a series of scenarios that will let you develop strategies for network deception attack and defense. You will work through Web attacks, and explore using deception to market an idea.

Track: Technology for Commerce and Military Defense

3:30 PM - 5:00 PM

27: Targeting Ourselves: IO and IW Education and Training

Chairman: Dr. Andrew Rathmell, Department of War Studies at King's College London; Dr. Dan Kuehl of the Information Operations Department at National Defense University; Lt. Col. Gregg Garrison, USAF

In this session Dr. Andrew Rathmell will take a look at the training efforts underway in the UK. Dr. Dan Kuehl will outline government education initiatives underway in the US and Lt. Col. Gregg Garrison, USAF, will discuss tactical-level skills training.

Track: Infowar: The Human Dimension

3:30 PM - 5:00 PM

28: Chinese Information Warfare

Lt. Col. Timothy L. Thomas, US Army, (Ret.), Analyst, US Army Foreign Military Studies Office, Fort Leavenworth; Adjunct Professor, US Army's Eurasian Institute, Germany

Lt. Col. Thomas will address the development of Chinese IW theory from 1995-present. He will focus on Chinese interpretation of U.S. actions in Kosovo and the Gulf War, and the Internet battle they conducted with Taiwan before the Taiwanese elections. He will cover the use of the Internet in Chinese society, and include a review of Chinese PSYOPS.

Schedule

Monday, September 11, 2000

Optional, One-Day Workshops

9:00 AM - 5:00 PM

W1 Legal Issues in Cyberspace and the Use of Force
W2 Countering the Dangerous IT Insider
W3 Everything You Wanted to Know About Global IW but Were Afraid to Ask
W4 Running a Successful Computer Crime Investigation and Prosecution
W5 Hacking 201
W6 The Essentials of Building ISACs

Thursday, September 14, 2000

9:00 AM - 5:00 PM

W7 Maintaining Real-Time Operational Continuity: The Fusion of Cyber Defense and Disaster Recovery
W8 Beyond Open Source: The Real Intelligence Revolution
W9 The ABCs of PKI
W10 Spying on Your Competitors: Legal Industrial Espionage
W11 Information Warfare: A Winning Tool for 2000 and Beyond
W12 Signals vs. Noise: Retrieving Important Information

Tuesday, September 12, 2000

7:00 - 8:15 AM Continental Breakfast and Early Registration

8:15 - 8:30 AM
Welcoming Remarks

8:30 - 9:00 AM
Keynote Address
What's Hot in Computer Crime in the Department of Justice

9:00 - 9:30 AM
Keynote Address
Privacy Concerns

Plenary Sessions

9:30 - 10:00 AM
1 Asymmetric Threats

10:00 - 10:30 AM Break

10:30 - 11:00 AM
2 The Human Factor in Infowar

11:00 - 11:30 AM
3 The Economics of Information Security

11:30 AM - 12:00 PM
4 Taking It to the People: National Security Awareness

12:00 - 1:30 PM Luncheon and Exhibits

12:30 - 12:45 PM
Luncheon Address
Distributed ACCRUAL of Service (DAOS) Attacks

Concurrent Sessions

1:30 PM - 3:00 PM
5 Law Enforcement's Role in Incident Response
6 Cyberweapon Control
7 Superterrorism in the 21st Century: WMD and Cyberterrorism

1:30 - 5:00 PM
8 The New Face of Economic Espionage: Offense and Defense in the Infosphere

1:30 - 3:00 PM
9 Introduction to Perception Management for the Warfighter
10 Waging Public Relations

3:00 - 3:30 Breaks and Exhibits

3:30 - 5:00 PM
11 Practical Law Enforcement vs. Ineffectual Policies
12 Information Assurance: Protecting Information Assets and Establishing Trust in a Networked Society
13 Operational Security
14 Critical Infrastructures: Human Perspectives
15 How Much Civil Liberty and Privacy Do We Have to Give Up to Gain Cyber Defense?

5:00 - 7:00 PM Reception/Expo

Wednesday, September 13, 2000

7:00 - 8:30 AM Continental Breakfast

8:30 - 9:00 AM
Keynote Address
Infrastructure Protection and National Security: A Legislative Review

9:00 - 9:30 AM
Keynote Address
Current Initiatives in the CIAO

9:30 - 10:00 AM
Keynote Address
Defending America's Cyberspace

10:00 - 10:30 AM Break

Plenary Sessions

10:30 - 11:00 AM
16 Chinese IW 101

11:00 - 11:30 AM
17 Creating Private-Sector National Cybersecurity: Five Necessary Steps

11:30 AM - 12:00 PM
18 The New Information Warfare Paradigm

12:00 - 1:30 PM Luncheon and Exhibits

Concurrent Sessions

1:30 - 3:00 PM
19 Privacy vs. Security: What Is the Government Doing to Help Us?
20 Active Defense Technologies
21 Modeling the Cyberterrorist's Behavior
22 The Media and Inforwar Hype
23 Perception Management for the Warfighter: Soft Weapons

1:30 - 5:00 PM
24 Infrastructure Studies

3:00 - 3:30 PM Break and Exhibits

3:30 - 5:00 PM
25 Organized Crime's Role in IW
26 Using Deception in Network Defense
27 Targeting Ourselves: IO and IW Education and Training
28 Chinese Information Warfare

5:00 - 5:15 PM
Conference Wrap-Up

5:15 - 6:30 PM Reception

Registration Information

Mail: the registration form to MIS Training Institute, 498 Concord Street, Framingham, MA 01702-2357
Call: (508) 879-7999
Fax: (508) 872-1153
E-mail: mis@misti.com
Web: www.misti.com

Times
Registration desk: Monday 8:00-9:00 am for workshops; Monday 5:00-7:00 pm; and Tuesday at 7:00 am.

Fees
Conference: $995
Conference and one workshop: $1290
Conference and two workshops: $1535
Workshop only: $395
All fees are payable in advance in US dollars. Fees include session materials; refreshments; lunch; continental breakfasts; and receptions on Monday, Tuesday, and Wednesday. Workshop fees include lunch, refreshments, and materials for the workshop(s) you attend.

Government Rates
Conference: $895
Conference and one workshop: $1160
Conference and two workshops: $1405
Workshop only: $295
Cannot be combined with other discounts.

Team Discount
When four people from your organization attend, each will receive a 20% discount. Registrations must be made and paid for at the same time. Cannot be combined with other discounts.

Continuing Education Credits
Participants are eligible to receive 15 hours of Continuing Education Credits for the conference, and an additional 7 for each workshop.

Accommodations
InfowarCon 2000 will be held at the Renaissance Washington, DC Hotel where a block of rooms has been reserved until August 19, 2000. After that date, reservations may be made on a space-available, regular-rate basis. **Make your reservations early and mention MIS/InfowarCon to be assured a room at the special rate.** To book your reservation, write the **Renaissance Washington, DC Hotel**, 999 9th Street, NW, Washington, DC 20001 or call (202) 898-9000.

Travel Discounts
Attendees are guaranteed lowest available airfares by using Abacus Travel, Inc. For information call Abacus at (877) 518-9867 and be sure to mention that you are attending *InfowarCon 2000*.

Cancellation
You may cancel your registration up until two weeks before the conference. For cancellations made within ten business days of the conference there is a $95 fee which will be waived if you register for another MIS program at that time. You may, at any time, substitute another individual from your organization. Those who do not cancel and do not attend will be responsible for the full fee.

Registration

InfowarCon *2000*

Conference & Expo
September 12-13, 2000
Washington, D.C.

Optional Workshops
September 11 & 14

☐ Yes! Please sign me/us up! (Photocopy for additional registrations)

Priority Code:

Name ☐ Mr. ☐ Ms. ☐ Mrs. ☐ Dr. ☐ Prof.

for Name Tag

Title | Organization

E-Mail Address (Required)

Industry | No. of Employees

Address | Mail Stop/Floor

City

State/Province | Zip/Mail Code

Phone | Fax

Approving Manager | Title

Priority Code: IW2K/2X/ H

Payment

☐ Conference $ .....
☐ Conference & one workshop $ .....
☐ Conference & two workshops $ .....
☐ Check enclosed (payable to MIS Training Institute) $ .....
☐ Bill me/my organization
P.O. # ..... PERC # .....
☐ Charge to my: ☐ VISA ☐ MasterCard ☐ AMEX

Account No. | Exp. Date

Signature

Cardowner's Name

I am unable to register, but please send me:

☐ Catalog of information security and audit seminars
☐ Free *TransMISsion Online* Audit & Security Newsletter
☐ Information about information security evaluations and strategic gaming from Interpact, Inc.

☐ Please add the above name or make the above correction to your mailing list.

☐ Please do not allow my name to be used by other companies.

Session Selections (circle one in each block)

Tuesday, 1:30-3:00	5 6 7 9 10	Wednesday, 1:30-3:00	19 20 21 22 23
Tuesday, 1:30-5:00	8	Wednesday, 1:30-5:00	24
Tuesday, 3:30-5:00	11 12 13 14 15	Wednesday, 3:30-5:00	25 26 27 28

Workshop Selections (circle one in each block)

Monday Workshops W1 W2 W3 W4 W5 W6
Thursday Workshops W7 W8 W9 W10 W11 W12

MIS TRAINING INSTITUTE
498 Concord Street
Framingham, MA 01702-2357

Fax (508) 872-1153 Call (508) 879-7999
E-mail: mis@misti.com Web: www.misti.com

REGISTER www.misti.com ON THE WEB!