InfowarCon™ 2001

September 5-6, 2001 *Washington, DC*

Optional Workshops *September 4 & 7*

Vendor Expo *September 5 & 6*

Techniques and Strategies for Securing Shared Infrastructures

FEATURED SPEAKERS...

- **The Honorable Tom Tancredo,** *US House of Representatives*
- **Ron Dick,** *Director, National Infrastructure Protection Center*
- **Gloria Craig,** *Director General, Security & Safety Ministry of Defence, UK*
- **Commodore Patrick Tyrell,** *Defence Communications Service Agency, UK*
- **Shunji Yanai,** *Japanese Ambassador to the United States*
- **General Dave Bryan,** *US Army; Commander, Joint Task Force Computer Network Operations; Vice Director, DISA*
- **Maarten Botterman,** *Director, ICT Policy Research; Project Coordinator, EU-Funded DDSI*
- **Stephen R. Katz,** *Chief Information Security and Privacy Officer, Merrill Lynch*

MIS TRAINING INSTITUTE

The International Leader in Audit & Information Security Training

INTERFACT

CO-SPONSORED BY:

TERRORISM RESPONSE ASSOCIATION INTERNATIONAL

SPONSORING PUBLICATIONS

INFORMATION SECURITY

FederalComputerWeek

EDUCATION PARTNER

AUERBACH

(ISC)² International Standard for Information Security

www.misti.com

E-Z ACCESS IW01

WELCOME TO InfowarCon™ 2001

Michael I. Sobol, CISA
Chairman
MIS Training Institute

Winn Schwartau
President
Interpact, Inc.

Chinese hackers deface US government Web sites. DDoS attacks are aimed at the White House Web site. Palestinian and Israeli hackers carry out cyber-skirmishes. With cyber-attacks, technical sabotage, and international acts of terrorism on the rise, mission-critical infrastructures have never been more vulnerable.

A Conference for the Times...

That's why *InfowarCon 2001* has been developed to deliver proven techniques and strategies for protecting your shared infrastructures from external and internal attack.

Now in its 12th year, this critically acclaimed event brings together military leaders, political forces, academics, and industry captains from all over the globe who will share their hard-won experiences and expertise. You will benefit from the first-hand knowledge of in-the-trenches infowarriors from such highly regarded organizations as the Carnegie Mellon Research Institute; UK Ministry of Defence; the Joint Military Training Center; Logicon; TNO Physics and Electronics Labs, Netherlands; Defence Communications Services Agency, UK; the National Infrastructure Protection Center; and more.

...And Topics That Hit the Mark

InfowarCon 2001 will arm you with the tactics you need to detect, react to, and protect against cyber-attacks. In session after session, you will learn the most up-to-date information warfare strategies and cover such topics as war in the age of the cyborg, targeting belief systems, cyber-diplomacy, state infrastructure protection centers, protecting telecom infrastructures, law enforcement counter-ops, and much more.

And, to help you focus on the areas in which you are most interested, sessions are slotted into six, targeted tracks:

- IS — *Information Space*
- T — *Technical*
- NIP — *National Infrastructure Protection*
- PPS — *People Problems & Solutions*
- LE — *Law Enforcement*
- IPS — *International Problems & Solutions*

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.

We look forward to being your host in Washington, DC.

Sincerely,

Michael I. Sobol, CISA
Chairman
MIS Training Institute
www.misti.com

Winn Schwartau
President, Interpact, Inc.
www.interpactinc.com
www.infowar.com

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

Why You Should Attend InfowarCon 2001

You will:

1. Take a peek at the **future of information warfare and how cyborg-style technology** can be used to make people vulnerable to perception control
2. Consider practical strategies for **minimizing cyber-risk to large telecommunications infrastructures**
3. Demystify the use of **national and international media** to disseminate and publicize government policies, actions, and intentions
4. Get an insider's view of how the **security culture of the British Ministry of Defence** is changing
5. Find out how traditional **methods and mechanisms used in the ancient art of deception** are being used in the cyber and digital realms...and how to protect against them
6. Get a primer on **handling cyber-crimes** and learn how local police and corporate citizens can work together
7. Delve into basic types of **government psychological operations programs that target belief systems**
8. Discover why **PSYOPS** is important to law enforcement organizations
9. Examine **threats from cyber-terrorists, including "hacktivists,"** and what you can do to combat them
10. Focus on the need for America to develop a cohesive strategy for **developing and implementing a quality IT manpower training program**
11. Evaluate how the US stacks up against other developers of **SIGINT**
12. Master techniques for **determining the motivation and allegiances of your employees**
13. Determine why and how **software engineering and network architecture** are inherently defective and hear one presenter's controversial solution
14. Cover the **legal restrictions imposed on local cyber-investigations**
15. Capitalize on **techniques Sweden has used to organize a national IO-D/CIP management effort**
16. Investigate the **ways public and private diplomacy are migrating into the realm of cyberspace**
17. Hear from the co-author of Arizona's **Statewide Infrastructure Protection Center (SIPC)** bill how such a center will work and why it is important
18. Explore **behavioral analysis of operation code** as a way to detect anomalies
19. Find out how to use **"sandboxing"** to minimize most forms of malicious code
20. Examine the realities of **CNA and the barriers to successfully employing its capabilities**

You will benefit from:

A Faculty of Hands-On Experts

You'll get proven techniques and broad perspectives from presenters who are in-the-trenches pros from the military, private, and political arenas.

Six Special Tracks

To make sure you optimize your conference experience and meet your objectives, we've organized *InfowarCon 2001* into six, targeted tracks:

Information Space: *Chaired by D.H. Dearth, Course Director, JMITC*
Sessions in this track examine the distinct mechanisms that help shape Information Space.

National Infrastructure Protection: *Chaired by Clayt Lemme, Supervisory Special Agent and Unit Chief, National Infrastructure Protection Agency*
This track delivers the basics of international infrastructure policies and procedures and the lessons learned.

Law Enforcement: *Chaired by Robert C. Rusnak, Senior Information Operations Analyst, Systems Technology Associates*
Sessions in this track look at the application of IW to law enforcement.

Technical: *Chaired by Winn Schwartau, President, Interpact, Inc.; Founder, NiceKids.Net and Infowar.com*
You'll find sessions in this track on advanced research and case studies from international experts in a variety of disciplines.

People Problems & Solutions: *Chaired by Morgan Wright, Deputy Director, Information Security, Federal Government Group, Unisys Corporation*
This new track is designed to give insights into various people problems…from leaders to kids.

International Problems & Solutions: *Chaired by Matthew Devost, Founding Director, Terrorism Research Center, Inc.*
From cooperative IO/IW to terrorism, the international community has a lot offer. The disparate sessions in this track cover the gamut of thinking and future ideas and capabilities.

Complete Conference Materials

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

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. *This savings cannot be combined with other discounts.*

"NETOPPS"

Networking opportunities abound at *InfowarCon 2001*. 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 2001* let you leverage your travel time and take advantage of an intensive day of learning.

Continuing Education Credits

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

Tuesday, September 4

9:00 AM - 5:00 PM

W1
Hacking 101: Tools and Techniques

Tim Rosenberg, J.D., White Wolf Consulting; Erik Naylor, Ph.D., White Wolf Consulting; Scott Zimmerman, Research Associate, Carnegie Mellon University's Software Engineering Institute

In this popular workshop you will explore hacking tools and techniques and learn the methodology behind hacking. You will cover target reconnaissance, vulnerability mapping, port scanning, password cracking, Trojan horse programs, and denial-of-service attacks, along with countermeasures for thwarting them. Using hacking tools in a safe environment, you will gain an understanding of common threats to the IT infrastructure. Demo computers and scattered attack/defend laptops will let you view countermeasures in action. You will have access to a Web site that has additional information in support of this workshop.

W2
Interviews and Investigations: Human Factors and Cyber-Crime

Morgan Wright, Deputy Director, Information Security, Federal Government Group, Unisys Corporation

In this workshop you will learn techniques that will help you screen for potential employees who would do you harm and gain strategies for investigating cyber-crimes. You will explore pre-employment interviews, behavioral analysis, insider profiling, and exit interviews as methods you can use to avoid being victimized by people you trust. You will review investigative tactics that can be applied to technology-related offenses, including criminal, civil, and accepted policy-use violations. You will discover how to conduct field forensics and collect and safeguard evidence, and learn specific techniques designed to elicit admissions of wrongdoing.

W3
Twisted Technology: The Dark Side of Enabling Technologies

Rusty Miller, President, Nemesis Technologies; Dr. Stephen Thaler, President, Imagination Engines, Inc.

In this workshop you will discover how computer and network technologies can be "twisted" to enable clandestine communications, surreptitious entry and control of computers and networks, advanced digital deception, Web-based PSYOPS, perception management, and digital anonymity. You will learn how twisted technologies will impact government and commercial information assurance strategies. You will find out how recent breakthroughs in A.I. will enable intrusion detection, digital deception and counterdeception, intelligence analysis and data mining, infrastructure attack and defense, and automated examination of program source code and mobile code for embedded malicious capabilities.

W4
Global Information Warfare and Information Operations: Perspective 2001

Lt. Col. Perry Luzwick, USAF (Ret.) and Director Information Assurance Architecture, Logicon Inc.; Andy Jones, Group Manager, Secure Information Systems, DERA, UK; George Kalb, Exploitation Expert, Northrop Grumman and Professor, Johns Hopkins University Graduate School

Geared to both industry and government, this unclassified workshop takes an intensive look at the global (conflict) playing field and delivers immediately applicable and useful strategies for defending it. You will learn who the new international players are, why we need to worry about them, their capabilities, and the threats they pose to us and to the infrastructures supporting our society. You will cover knowledge management and how to take advantage of the entire spectrum of information to make informed decisions to speed up the OODA loop process–for peace, business and conflict. You will discover how the bad guys exploit systems and find out what can you do about it...quickly.

W5
Building and Securing Wireless Networks for Government, Business, and Conflict

Paul Zavidniak, Member of Technical Staff, Logicon, Inc.; Bob Husnay, Air Force Research Labs, Rome Labs; Steve Wilson, Program Manager, SAIC; Tim Havighurst, NSA

As communications and the Internet go wireless, the security frontier becomes inherently more dangerous. In this timely workshop you will examine new threats to business and government, the technology plans and strategies that make sense today, and countermeasures for mitigating these new risks. You will get the US military perspective on wireless communication systems, and gain insights into their vision, where they see risks, and the programs they have in place to thwart them. You will explore leading-edge R&D programs detailing concepts and approaches designed to help the DoD protect against these risks. You will cover wireless intrusion detection and the detection of wireless-based denial-of-service attacks. You will gain an understanding of the security risks inherent in COTS solutions, and discover why leading-edge R&D is essential if we are to operate over-the-air in a hostile environment. You will also find out how any over-the-air communications medium can be exploited by anyone intent on using data for personal, business, group, or national objectives.

"...If a well-funded, organized series of cyber-attacks were to strike a target's economic and structural nerve centers, it would send the target society into chaos and make it difficult for the military to communicate and move troops."

–Computerworld, January 24, 2001

W6
The Role of Information Warfare: The Balance of Power in the Coming Century

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

In this workshop you will learn how information warfare can be applied by the world's armed forces to change the balance of power in the coming century and the techniques that will accomplish this. You will discover the primary forces pushing the world's military to employ information warfare techniques. You will learn ways to predict how certain immutable physical laws limit weapon system performance, and investigate a powerful and freely available tool that can ensure communication security. You will get a peek at possible radical changes in the direction US military forces will take in the near future and review the application of advanced predictive computer programs that reveal both weapons and human performance in combat.

Friday, September 7

9:00 AM - 5:00 PM

W7
Computer and Network Forensics 101 for Law Enforcement Professionals and Investigators

Mike Anderson, President, New Technologies, Inc.

In this detailed workshop you will explore the basics of technical cyber-crime investigations. You will see firsthand how forensics tools work, learn the tricks that the bad guys use, and gain techniques for uncovering their tracks. You will determine how your computers and networks can be manipulated and how to get the evidence you need to establish a cyber-crime has taken place. You will discover how to find "computer secrets" and weaknesses in DOS, Windows®, Windows 95, Windows 98, Windows NT®, and Windows 2000, and to track down computer evidence and computer security data leakage.

W8
Chinese and Russian Information Warfare

Lt. Colonel Timothy L. Thomas, US Army (Ret.); Analyst, Foreign Military Studies Office, Ft. Leavenworth

In this one-day, eye-opening workshop you will get a guided tour of the recent advances in Chinese and Russian infowar. You will examine some of the new developments in theory, what Russian cyberspace looks like, the reconnaissance-strike complex, and IO. You will cover Russia's new information security doctrine and its Institute of Systems Analysis: Center of Creative IW Thinking, including information weapons and PSYOPS. You will examine risk aversion and risk management, and the impact of information technologies on deterrence from US, Russian, and Chinese viewpoints.

W9
Legal Issues in Computer Network Operations and the Use of Force in Cyberspace

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

In this revealing workshop you will focus on the legal implications of computer network operations and the use of force in cyberspace. You will learn about the US Department of Defense war-fighting organization for Computer Network Operations and explore what information operations warfighters/operators and their legal advisers should consider before engaging in warfare in cyberspace. In a series of interactive presentations you will define an analytical legal framework. Using case studies, you will explore such critical issues as what constitutes the use of force in cyberspace, what cyberspace activities are legal and illegal under the law of armed conflict, and when hacking-back and shooting-back are lawful.

W10
Hacking 201: Advanced Tools and Techniques

Tim Rosenberg, J.D., White Wolf Consulting; Erik Naylor, Ph.D., White Wolf Consulting; Scott Zimmerman, Research Associate, Carnegie Mellon University's Software Engineering Institute

Designed for those with a solid background in IP networking, this penetrating workshop will cover advanced hacking methods in a multi-operating system environment. You will explore complex reconnaissance methods, privilege escalation, buffer overflows, distributed denial-of-service attacks, advanced Trojan horse use, file hiding through steganography, and dealing with logs. You will review wireless security and protocols and possible compromise points, and in a demonstration environment, you will use scattered laptops that will allow you to chat with each other and the instructors through IRC and e-mail. In-class demos will give you firsthand experience with the tools and methods of the workshop.

W11
Secure E-Mail in 5,000 Easy Lessons

Lawrence Hughes, Founder, CipherTrust; Author, Internet E-Mail: Protocols, Standards and Implementation

In this technical workshop you will explore how to secure Internet e-mail using the IETF standards. You will cover e-mail vulnerabilities, symmetric key and public key crypto, message digests, digital signatures, digital envelopes, and public key digital certificates. You will also look at PKI, CRLs, OCSP, LDAP, PGP, S/MIME, SSL/TLS, server certificates, SMTP over SSL, POP and IMAP over SSL, Webmail, secure remote administration with strong client authentication, and putting it all together in an appliance based on hardened Unix. You will investigate the use of a secure e-mail proxy to add security to a legacy e-mail server and view an e-mail hacking demo. The technical level of this workshop is fairly high.

Wednesday, September 5

8:15 AM - 8:30 AM

Welcoming Remarks

8:30 AM - 9:00 AM

Keynote: A Political View

The Honorable Tom Tancredo (R-CO), US Congress

9:00 AM - 9:30 AM

Keynote: A Military View

General Dave Bryan, US Army; Commander, Joint Task Force Computer Network Operations; Vice Director, DISA

9:30 AM - 10:00 AM

Keynote: A Legal View

Ron Dick, Director, National Infrastructure Protection Center

10:30 AM - 11:00 AM

Keynote: A Private Sector View

Howard Schmidt, Chief Security Officer, Microsoft Corporation

In his keynote address Howard Schmidt will reveal the factors that go into making security a successful part of an organization. He will also explore the threats that face organizations today and the steps they can take to protect against them.

1 11:00 AM - 11:30 AM

UK MoD: Protecting the Fortress

Gloria Craig, Director General, Security & Safety, Ministry of Defence, UK

In this stimulating session you will get an insider's view of how the security culture of the British Ministry of Defence (MoD) is changing as a result of two forces: Director General Craig's efforts to internalize security and make it part of core business; and inevitability, as the MoD links up to the outside world and moves from an IT fortress to a more dynamic, time-based approach. You will look at some of the issues raised by new British legislation, including the new Data Protection Act and Freedom of Information Act, and how the British protect their information. You will also examine the problems of older legislation in this context.

2 11:30 AM - 12:00 PM

The People vs. Technology: Assuring Information Assurance

Winn Schwartau, President, Interpact, Inc.; Founder, NiceKids.Net and Infowar.com

Would you let just anyone run around your company's offices? Of course not! How about your unclassified facilities? No way! Yet defense and private organizations are doing just that. In this authoritative session you will learn techniques that will help you know more about who you've hired, and how to determine their motivations and allegiances.

12:00 PM - 1:30 PM

Luncheon Address: How Much IA Spending Is Really Going On?

Dennis McCallam, Member of the Technical Staff, Logicon, Inc.; Representing GEIA

In this luncheon address Dennis McCallam will take a humorous look at the size of the information assurance market for defense and civil agencies.

3 IS 1:30 PM - 3:00 PM

Artists, Artistry, and Deceivers

Douglas H. Dearth, Course Director, Joint Military Training Center; Rusty Miller, President and CEO, Nemesis Technologies; Professor Bill Hutchinson, Associate Head, Cowan University, Australia

In this thought-provoking session you will explore the traditional methodologies and mechanisms used in the ancient art of deception. You will discover how these traditional concepts are being employed in the cyber and digital realms, and what you can do to protect your organization from them.

4 NIP 1:30 PM - 3:00 PM

NIPC Update: Operational Successes and Failures

A. Brett Hovington, Supervisory Special Agent, National Infrastructure Protection Center

Well into its fourth year, the FBI's National Infrastructure Protection Center continues to grow and expand its efforts in infrastructure protection. In this session you'll get an insider's look at its workings, its current focus, and its latest successes.

5 LE 1:30 PM - 3:00 PM

What Local Cops Need to Know About Cyber-Crime

Howard Schmidt, Chief Security Officer, Microsoft Corporation

This incisive session is a primer on handling a cyber-crime. You will learn how local police and corporate citizens can work as partners–not adversaries–in solving cyber-crimes. You will cover computer network defense, network attack, intrusion detection, reaction, and time-based security.

6 T 1:30 PM - 3:00 PM

The Broken Bit

Eric Luiijf, Principal Consultant, Telecommunications and Security Division of the TNO Physics and Electronics Laboratory, Netherlands

The TNO initiated a study to investigate how different layers of organizations are interrelated with one another and the Internet. In this session you will review the ongoing results of this international study to gain a deeper understanding of the taxonomies and tools required to evaluate interorganizational responsibilities. You will look at the many ways that the Internet is vulnerable and investigate how these vulnerabilities affect private and public organizations and responsibility for survival.

7 PPS 1:30 PM - 3:00 PM
Why Government System Security Is Still a Failure

Chey Cobb, Former Senior Technical Security Advisor, National Reconnaissance Office

Attend this dynamic session for some surefire controversy! Chey Cobb, one of the founding employees of the National Computer Security Association (now ICSA) and a former security officer for the NRO, will reveal the reasons why government security efforts are ineffective. You will find out why the top brass can't see the need for security, why security budgets are so low, and why the worst offenders are senior leaders who think they don't have to follow the rules.

8 IPS 1:30 PM - 3:00 PM
Cyber-Terrorism: Who, When, and Why

Matthew G. Devost, Founding Director, Terrorism Research Center, Inc. and Director of Operations, Security Design International; Robert E. Stevens, Senior Technical Manager, Special Projects Department, ITT Industries, Advanced Engineering & Sciences Division

In this session you will examine cyber-terrorism threats, including the emerging "hacktivist." You will discover why terrorists are using information attacks, what they are targeting, and how government, law enforcement, and industry can identify, protect against, and respond to these threats. You will learn how conventional and neo-terrorists have migrated to cyberspace, who these groups and individuals are, and why they are resorting to these methods. You will find out what the experts and studies are saying about when significant cyber-terror acts will occur. You'll also delve into government response options, industry considerations, and lessons learned. Recent case studies of threat agents who have attempted to penetrate corporations that conduct terrorism research or provide support to the US government will give you a real-world view of this growing problem.

9 IS 3:30 PM - 5:00 PM
Targeting Belief Systems

Susan Driscoll, UK Ministry of Defence; Colonel Charles A. Williamson, USAF (Ret.), Office of the Assistant Secretary of Defense, Special Operations and Low Intensity Conflict; Robert Garigue, Vice President, Information Security, Bank of Montreal Group of Companies

Successful PSYOPS and deception programs depend on targeting, conditioning, and influencing the belief systems of specific individuals and groups. In this breakthrough session you will get a political, military, and industry look at these undertakings from in-the-know insiders. Susan Driscoll will outline the complex psychological principles and processes involved in PSYOPS and deception. Col. Charles Williamson will cover basic types of government psychological operations programs that target belief systems. Robert Garigue will take the session into the realm of cyberspace as he explores hacking belief systems.

10 NIP 3:30 PM - 5:00 PM
International Cooperation, EU Efforts, and Law Enforcement

Clayt Lemme, Supervisory Special Agent and Unit Chief, National Infrastructure Protection Center

Cooperation among law enforcement agencies from multiple countries has resulted in a majority of the successful efforts against today's cyber-threats. In this timely session you will walk through cases that required extensive international law enforcement cooperation and learn the steps that the NIPC is taking to build greater cooperative efforts in the future.

11 LE 3:30 PM - 5:00 PM
Law Enforcement Counter-Operations, PSYOPS, and Perception Management

Robert C. Rusnak, Senior Information Operations Analyst, Systems Technology Associates

In this fast-paced session you will find out why PSYOPS is important to law enforcement and what it can do to help law enforcement organizations. You will determine how it can affect demonstrations, the demonstrators themselves, the media, and public perceptions. You will learn why IO campaign planning is critical to success and get tips on getting buy-in from your chief of police and/or mayor.

12 T 3:30 PM - 5:00 PM
Applying Unmanned Vehicle Technologies to Information Warfare, Operations, and Law Enforcement

Jay R. Snyder, Chief Operating Officer, Victory Systems, LLC

The use of unmanned vehicles in law enforcement, the military, and government agencies is about to explode, and the next revolution will be robotics. In this session you will discover how the combination of new physical and intelligence technologies will open up an ever-expanding realm of possibilities for intelligence gathering and situation response. You will find out how unmanned vehicles will be used singularly, in groups, and in great architectures, and how vehicles, sensors, and non-lethal application of force can be mixed and matched to answer the needs of the mission.

13 PPS 3:30 PM - 5:00 PM
Has IT Manpower Training Become a Matter of National Security?

Professor William G. Perry, Ph.D., Professor, Business Computer Information Systems College of Business, Western Carolina University

There is now a documented shortage of qualified IT professionals in the US to help us maintain our preeminence as a global power. In this session you will focus on the need for America to develop a cohesive strategy for developing and implementing a quality IT manpower training program. You will define the severity of the problem, the fragmented efforts currently underway to alleviate the situation, and possible solutions for mitigating the IT training shortages at local, state, regional, and national levels.

14 PPS 3:30 PM - 5:00 PM
Conflict in the Age of the Cyborg: A Future View of Infowar

Dr. William Hutchinson, Associate Head, School of Management Information Systems, Edith Cowen University

In this thought-provoking session you will take a peek at the future of infowarfare and how cyborg-style technology can be used to make people vulnerable to ultimate perception control. You will examine the vulnerabilities of human/machine systems, including manipulation and destruction, and learn defense strategies against such systems. You will also investigate the social implications of human/machine systems.

Thursday, September 6

8:30 AM - 9:00 AM
Keynote: Japan, the G8, and International Cyber-Crime

Japanese Ambassador to the United States, Shunji Yanai, and/or Political Counselor Takashi Murata

With cyber-tensions high in the Pacific Rim, Japan has raised alerts to potential attacks on its government and business services. Now you can hear how Japan, as a G8 member, is also involved in global crackdown efforts against cyber-crime and child pornography. We are honored to have Japan's participation in *InfowarCon 2001*.

9:00 AM - 9:30 AM
Keynote: Creating a Dependable Information Infrastructure in Europe

Maarten Botterman, Director of ICT Policy Research , Project Coordinator of the EU- Funded DDSI, Leiden, The Netherlands

15 9:30 AM - 10:00 AM
Information Warfare: Brooding Nemesis or Paper Tiger?

Commodore Patrick J. Tyrrell, DCE, Defence Communications Services Agency, UK

In this penetrating session you will examine the real infowar issues governments and multi-national corporations will have to worry about in the future. You will determine how much of the hype is justified and what you should be doing in the next few years to make sure you are prepared for what's to come.

16 10:30 AM - 11:00 AM
Who's Protecting Our Economic Infrastructures?

Stephen R. Katz, Chief Information Security and Privacy Officer, Merrill Lynch

In this riveting session you'll get an industry captain's view of what it will take to make the economic sector safe from cyber-assault.

17 11:00 AM - 11:30 AM
Software Defects: Gateways to Cyber-Terrorism

Paul Strassmann, President, Strassmann, Inc.

In this session you will find out why and how existing software engineering and network architectures are inherently defective. You will focus on two key contributors to this situation: vendors who provide software that meets marketing needs and not user needs, and application designers who deliver software so complex that it cannot be protected.

18 11:30 AM - 12:00 PM
NSA and SIGINT Capabilities Today…and Tomorrow

Jim Bamford, Author, The NSA and SIGINT

Signals Intelligence (SIGINT) can provide a near real-time picture of enemy electronic emitters on the battlefield and provide the ability to detect, identify, locate, track, and attack user-selected electronics. Attend this session to find out how the US stacks up against other developers of SIGINT today…and in 2020.

19 IS 1:30 PM - 3:00 PM
Bits, Bytes, and Cyber-Diplomacy

Panel of Experts

Public and private diplomacy has always been among the most traditional government mechanisms in international politics and security affairs. In this intriguing session you will learn how this activity is migrating into the realm of cyberspace. You will benefit from the real-world experiences of a panel of serving diplomats who will share their ideas in a wide-ranging discussion.

20 NIP 1:30 PM - 3:00 PM
Legal Implications of Information Sharing

Steven R. Chabinsky, Assistant General Counsel, Federal Bureau of Investigation

If you provide proprietary information to the government, can it be protected from release to your competitors? What are the legal liabilities of providing information that turns out to be incorrect and that has been acted upon? Get the answers to these and other pressing information-sharing questions in this session.

21 LE 1:30 PM - 3:00 PM
Legal Issues or Law Enforcement: CNA and CND

Rich Aldrich, Judge Advocate General, AF/OSI; Commander Dave Pettinari, Pueblo County Sheriff's Office

In this information-packed session you will cover the legal restrictions imposed on local cyber-investigations. You will determine when the police should be involved and if they can legally do less than an individual or corporation can. You will explore the use of CNA/E in kiddy-porn investigations and the legal aspects of CNA/CND.

22 T 1:30 PM - 3:00 PM
Protecting Large Telecom Infrastructures and Countering Public Cellular Network Vulnerabilities

Ed Amoroso, Vice President, AT&T Network Security; Scott Forbes, Senior Technology Auditor, Internal Audit Department, Nextel Communications

In this session you will investigate practical strategies for minimizing cyber-risk to large telecom infrastructures. You will examine the vulnerability of commercial cellular networks to malicious attacks. You will identify key network risk areas found in commercial cellular systems, and consider a variety of solutions, including advanced ACK/NAK protocols and GPS; physical security standards; and SSL, Java, key management in WAP gaps, and near-horizon solutions-oriented technologies.

23 PPS 1:30 PM - 3:00 PM
Ethics as Part of a National Awareness Campaign

Winn Schwartau, President Interpact, Inc.; Founder, NiceKids.Net and Infowar.com

In the infowar arena, technology is the problem, not the solution. In this session you will examine this dilemma and explore the areas where we have fallen short: a lack of cyber-ethics and an understanding of the basics.

24 IPS 1:30 PM - 3:00 PM
Information Operations/Critical Infrastructure Protection: Swedish and Romanian Views

Lars Nicander, Secretary of the Cabinet WG on IO-D/CIP, National Office of IO/CIP Studies, National Defence College; Ltc. Eng. Drd. Vasile Paun, Romanian Ministry of Defence

Sweden has been prominent in the IW/IO field for years and especially astute about critical infrastructure protection. In this session you will find out how this small, highly Internet-connected country attempts to manage the new needs of cross-sector protection. You will cover organizing a national IO-D/CIP management effort and why it is important to coordinate it internationally. You will also hear why Romania views IW/IO as a holistic issue across its entire military capability.

25 IS 3:30 PM - 5:00 PM
Managing the Unmanageable

Paul Koring, Senior Editor, Toronto Globe and Mail

National and international media have long been among the primary mechanisms for disseminating and publicizing government policies, actions, and intentions. As a result, managing relations with the media is a primary concern of civil governments and their military establishments. Conversely, public media in democratic societies strenuously attempt to disassociate themselves from such governmental controls. In this session a panel of noted media and government experts will demystify the ins and outs of this dynamic process.

26 NIP 3:30 PM - 5:00 PM
Building an Information Sharing and Analysis Center

Peter Allor, Manager, MSS IT Analysis, ISS, IT-ISAC

An Information Sharing and Analysis Center (ISAC) is a forum for sharing best security practices among members. In this session you will get tips on forming such a group for the purpose of reporting, responding to, and developing trend analysis, and exchanging information about threats, attacks, and defensive measures for protecting critical infrastructures.

27 LE 3:30 PM - 5:00 PM
State Infrastructure Protection Centers

Jim Christy, Special Assistant for Law Enforcement, Information Assurance ASDC3I/IA

Arizona's Statewide Infrastructure Protection Center (SIPC) bill establishes a first-of-its-kind, state-level IT infrastructure protection center in the US. In this insider's session Jim Christy, co-author of the SIPC bill, will review the legislation, how the SIPC will work, and why it is so important.

28 T 3:30 PM - 5:00 PM
New Defensive Network Technologies and Approaches

John Munson, President, Cylant Corporation; Peter Privateer, President, Pelican Security

In this session you will explore behavioral analysis of operation code as a way to detect anomalies. You will learn how this technology works, why it has such a low performance hit, and why it is difficult to subvert.You will find out how sandboxing solutions work, and learn how corporate/government information operations can proactively protect, detect, and react to malicious code.

29 IPS 3:30 PM - 5:00 PM
Standardizing Immunity to High-Power Electromagnetic Transient Phenomena

Dr. William A. Radasky, President, Metatech Corporation, USA; Manuel W. Wik, Strategic Specialist, Defence Materiel Administration, Joint Materiel Command, Sweden

In this session you will pinpoint the new electromagnetic threats to civilian infrastructure and cover the worldwide standardization efforts of the IEC. You will learn about immunity to EMP from high-altitude nuclear explosions, HPM and UWB emitters, and how the work of the IEC can result in civilian standards.

30 IPS 3:30 PM - 5:00 PM
CNA: Beyond the Hyperbole

Matthew G. Devost, Founding Director, Terrorism Research Center, Inc. and Director of Operations, Security Design International

A Computer Network Attack (CNA) is a lot more than hackers downloading tools from the Internet. The US Government spends considerable sums developing such offensive cyber-weapons as part of an active defensive strategy. In this session you will look at the realities of CNA and the barriers to employing its capabilities.

SCHEDULE

Optional, One-Day Workshops

Tuesday, September 4, 2001

9:00 AM - 5:00 PM

W1 Hacking 101: Tools and Techniques

W2 Interviews and Investigations: Human Factors and Cyber-Crime

W3 Twisted Technology: The Dark Side of Enabling Technologies

W4 Global Information Warfare and Information Operations: Perspective 2001

W5 Building and Securing Wireless Networks for Government, Business, and Conflict

W6 The Role of Information Warfare: The Balance of Power in the Coming Century

Friday, September 7, 2001

9:00 AM - 5:00 PM

W7 Computer and Network Forensics 101 for Law Enforcement Professionals and Investigators

W8 Chinese and Russian Information Warfare

W9 Legal Issues in Computer Network Operations and the Use of Force in Cyberspace

W10 Hacking 201: Advanced Tools and Techniques

W11 Secure E-Mail in 5,000 Easy Lessons

Wednesday, September 5, 2001

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

8:15 - 8:30 AM Welcoming Remarks

8:30 - 9:00 AM Keynote: A Political View

9:00 - 9:30 AM Keynote: A Military View

9:30 - 10:00 AM Keynote: A Legal View

10:00 - 10:30 AM Refreshment Break

10:30 - 11:00 AM Keynote: A Private Sector View

Plenary Sessions

11:00 - 11:30 AM

1 UK MoD: Protecting the Fortress

11:30 AM - 12:00 PM

2 The People vs. Technology: Assuring Information Assurance

12:00 - 1:30 PM Luncheon

12:30 - 12:45 PM Luncheon Address: How Much IA Spending Is Really Going On?

Concurrent Sessions

1:30 - 3:00 PM

3 Artists, Artistry, and Deceivers

4 NIPC Update: Operational Successes and Failures

5 What Local Cops Need to Know About Cyber-Crime

6 The Broken Bit

7 Why Government System Security Is Still a Failure

8 Cyber-Terrorism: Who, When, and Why

3:00 -3:30 PM Refreshment Break and Exhibits

3:30 - 5:00 PM

9 Targeting Belief Systems

10 International Cooperation, EU Efforts, and Law Enforcement

11 Law Enforcement Counter-Operations, PSYOPS, and Perception Management

12 Applying Unmanned Vehicle Technologies to Information Warfare, Operations, and Law Enforcement

13 Has IT Manpower Training Become a Matter of National Security?

14 Conflict in the Age of the Cyborg: A Future View of Infowar

5:00 -7:00 PM Reception and Expo

Thursday, September 6, 2001

7:00 - 8:30 AM Continental Breakfast

8:30 - 9:00 AM Keynote: Japan, the G8, and International Cyber-Crime

9:00 - 9:30 AM Keynote: Creating a Dependable Information Infrastructure in Europe

Plenary Sessions

9:30 - 10:00 AM

15 Information Warfare: Brooding Nemesis or Paper Tiger?

10:00 - 10:30 AM Refreshment Break

10:30 - 11:00 AM

16 Who's Protecting Our Economic Infrastructures?

11:00 - 11:30 AM

17 Software Defects: Gateways to Cyber-Terrorism

11:30 AM - 12:00 PM

18 NSA and SIGINT Capabilities Today...and Tomorrow

12:00 - 1:30 PM Luncheon and Exhibits

Concurrent Sessions

1:30 - 3:00 PM

19 Bits, Bytes, and Cyber-Diplomacy

20 Legal Implications of Information Sharing

21 Legal Issues or Law Enforcement: CNA and CND

22 Protecting Large Telecom Infrastructures and Countering Public Cellular Network Vulnerabilities

23 Ethics as Part of a National Awareness Campaign

24 Information Operations/Critical Infrastructure Protection: Swedish and Romanian Views

3:00 - 3:30 PM Refreshment Break and Exhibits

3:30 - 5:00 PM

25 Managing the Unmanageable

26 Building an Information Sharing and Analysis Center

27 State Infrastructure Protection Centers

28 New Defensive Network Technologies and Approaches

29 Standardizing Immunity to High-Power Electromagnetic Transient Phenomena

30 CNA: Beyond the Hyperbole

5:00 - 6:30 PM Conference Wrap-Up and Reception

ABOUT...

MIS Training Institute

Now in its 23rd 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.

Interpact, Inc.

Interpact, Inc. is a security consulting organization specializing in penetration studies, security systems architecture, strategic gaming, and electronic civil defense.

Federal Computer Week

Federal Computer Week is the number one newsweekly in the federal information technology market. Published 41 times per year, FCW is read by more than 86,000 IT professionals in the federal government.

The High Tech Crime Network

Founded in 1991, The High Tech Crime Network is the leading independent certification body providing professional certification in the discipline of computer crime investigation and forensics to both the law enforcement and corporate sectors. The organization consists of over 1000 law enforcement officers and corporate information security professionals.

Terrorism Response Association International (TRAI)

TRAI is a professional association with members in the fields of law enforcement, public safety, fire services, corporate security, military, and government agencies. TRAI offers its members "real- time" information and alerts via the Internet, and sponsors terrorism response, security, and information security conferences and summits around the world.

Information Security Magazine

Information Security Magazine is the industry's leading trade publication, a one-step resource for news, analysis, insight, and commentary on today's infosecurity marketplace.

Auerbach

For 40 years, Auerbach has been the premier publisher for information technology professionals. Auerbach offers a wide range of publications, both print and electronic, including *IT Knowledgebase*.

(ISC)²

(ISC)² is an international organization dedicated to the certification of information systems security professionals and practitioners. (ISC)² grants the Certified Information Systems Security Practitioner (CISSP) designation.

InfowarCon Expo 2001

Check out the leading providers of security products and services at the vendor expo on Wednesday and Thursday. You will have the unique opportunity to network, ask questions, and see product demos! For an updated list of the outstanding organizations on board for this event, go to www.misti.com, enter E-Z Access: IW01, and click on "Conference Expo."

For information on how you can exhibit at this or other MIS Training Institute events, contact Adam Lennon at (508)879-7999 x336 or alennon@misti.com.

Conference Registration Information

Five easy ways to register:

Online: www.misti.com **E-Z Access IW01**

Mail: MIS Training Institute
498 Concord Street
Framingham, MA 01702-2357

Call: (508) 879-7999 x346

Fax: (508) 872-1153

E-Mail: mis@misti.com

Times

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

Fees

Conference: $1095 ***Conference + one workshop:*** $1490
Workshop only: $495 ***Conference + two workshops:*** $1835

All fees must be paid in advance in US dollars. Please add $100 administration fee if registering on or after August 29. Fees include Web access to session materials (excluding workshops), refreshments, lunch, continental breakfasts, and receptions on Tuesday, Wednesday, and Thursday.

Special Discounts

Government and Academia

Conference: $895 ***Conference + one workshop:*** $1190
Workshop only: $395 ***Conference + two workshops:*** $1465

These savings cannot be combined with other discounts.

Team

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

Students

Please call 508-879-7999, x346, to inquire about special rates.

Continuing Education Credits

Participants are eligible to receive 15 hours of Continuing Education Credits for the conference, and 7 credits for each workshop. If you are a CISSP, we will forward your credits to (ISC)².

Accommodations

InfowarCon 2001 will be held at the Renaissance Washington, DC Hotel, where a block of rooms has been reserved until August 12, 2001. After that date, reservations may be made on a space-available, regular-rate basis. Make your reservations early and be sure to mention MIS/*InforwarCon* to be assured a room at the special rate. To book your reservation, contact the Renaissance Washington, DC Hotel at 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. Call Abacus at 877-518-9867 and mention MIS/*InfowarCon*.

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 $100 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 are responsible for the full fee.

Guarantee

Attend this conference and gain contacts, strategies, and tools that will help you in your job. If you do not, simply tell us why on your company letterhead and we will give you a full credit toward another program or refund the fee.

InfowarCon™ 2001

September 5-6, 2001 *Washington, DC*
Optional Workshops *September 4 & 7*
Vendor Expo *September 5 & 6*

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

Name ☐ Mr. ☐ Ms. ☐ Mrs. ☐ Dr. ☐ Prof.

For Name Tag

Job Title | Organization/Company

E-Mail Address (Required)

Industry | No. of Employees

Address | Mail Stop/Floor

City

State/Province | Zip + 4/Mail Code

Phone | Fax

Approving Manager | Job Title

CISSP #_____

Payment

❑ Conference $_____ ❑ Conference & one workshop $_____
❑ Workshop only $_____ ❑ Conference & two workshops $_____
❑ Check enclosed *(payable to MIS Training Institute)* Amount $_____
❑ Bill me/my organization

P.O. #_____ PERC #_____

❑ Charge to my: ❑ VISA ❑ MasterCard ❑ AMEX

Account No. | Exp. Date

Signature

Cardowner's Name

WORKSHOP SELECTIONS *(circle one in each box)*

Tuesday, September 4, 9:00 - 5:00
W1 W2 W3 W4 W5 W6

Friday, September 7, 9:00 - 5:00
W7 W8 W9 W10 W11

SESSION SELECTIONS *(circle one in each box)*

Wednesday, September 5, 1:30 - 3:00
3 4 5 6 7 8

Wednesday, September 5, 3:30 - 5:00
9 10 11 12 13 14

Thursday, September 6, 1:30 - 3:00
19 20 21 22 23 24

Thursday, September 6, 3:30 - 5:00
25 26 27 28 29 30

I am unable to register, but please send me:

❑ *Catalog of Information Security and Audit Seminars*
❑ Free *TransMISsion Online Newsletter*
❑ Information about infosecurity evaluations and strategic gaming from Interpact, Inc.
❑ Information on CISSP certification for security professionals
❑ **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.**

498 Concord Street, Framingham, MA 01702-2357
Phone: (508) 879-7999 *Fax:* (508) 872-1153
E-mail: mis@misti.com

www.misti.com
E-Z ACCESS IW01

498 Concord Street
Framingham, MA 01702-2357

PRSRT STD
U.S. POSTAGE
PAID
PERMIT #17
LEOMINSTER, MA

Priority Code: IW01/ 2X / 5 / 6 / H