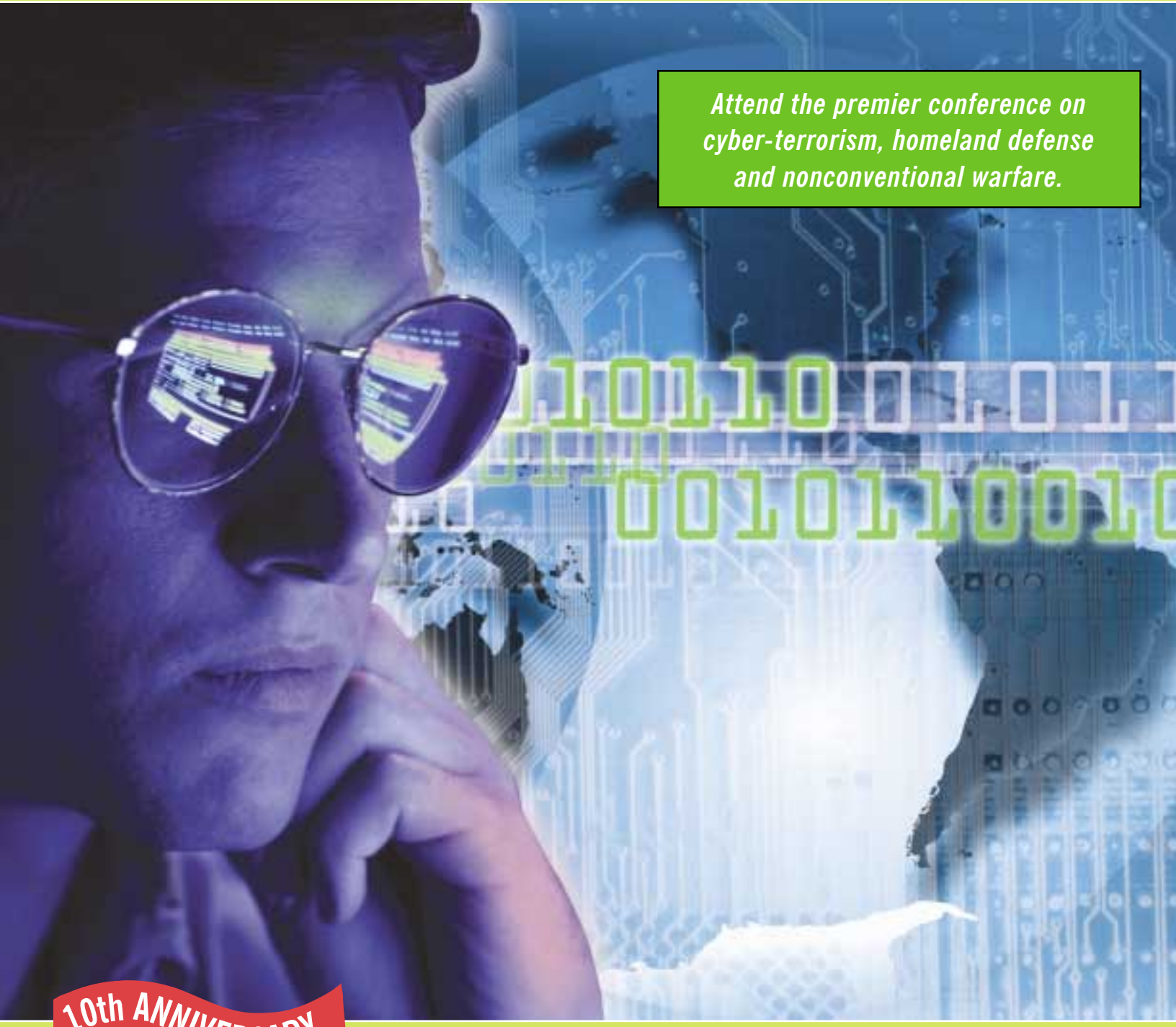
LEARN THE TACTICS AND TECHNOLOGIES OF DIGITAL WARFARE.



10th ANNIVERSARY

InfowarCon™

September 30–October 3, 2003 | Renaissance Washington D.C. Hotel | Washington, D.C.

Register today at www.infowarcon.com or call 800-875-7556

Produced and managed by:

Reed Exhibitions

TRC 2003

Co-located with:

TRC 2003

ANNUAL COUNTERTERRORISM & HOMELAND SECURITY CONFERENCE & EXPO

October 1–3, 2003

The Terrorism Research Center's Annual Conference and Expo on Counterterrorism and Homeland Security provides an unparalleled insider's perspective on the war against terrorism. The hard-hitting conference sessions cover critical topics including:

- Understanding the Terrorist Mindset
- Al Qaeda 2005
- Fourth Generation Warfare: Implications for Law Enforcement and Homeland Security

See inside for more details!

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
- CEOs, CTOs, managing directors
- IS directors, managers/staff
- MIS managers
- Legal counselors
- Law enforcement officers
- Computer crime investigators
- Security consultants
- Network security architects
- Network/LAN administrators
- Systems analysts/administrators
- IT auditors
- Information systems managers
- Academics in computer science/IW strategic studies

…and anyone responsible for enterprise and infrastructure information assurance and operations

Vendor Expo

See the most innovative homeland security and law enforcement technologies and equipment at the vendor expo on Wednesday and Thursday. Put new solutions to the test and network with your peers and industry experts.

KEYNOTE PRESENTATIONS— Experts from the worlds of government, intelligence and the military

For both InfowarCon and TRCcon, we've secured an outstanding roster of keynote speakers. Each is an expert in his field—and each presentation is free to all badged attendees. Here's a sampling of the luminaries you'll see:

- Paul B. Kurtz, Special Assistant to the President and Senior Director for Critical Infrastructure Protection, The White House
- Lowell E. Jacoby, USN, Director, Defense Intelligence Agency
- Congressman Jim Turner (TX-D), Ranking Member, Committee on Homeland Security
- Ralph Basham, Director, United States Secret Service
- Brig. Gen. Jack J. Catton, Deputy Director for Information Operations
- Brian Michael Jenkins, RAND Corporation
- Winn Schwartau, Founder InfowarCon
- Douglas Dearth, Co-Chair InforwarCon

Register today at **www.infowarcon.com**.

10th ANNIVERSARY

InfowarCon™

September 30 – October 3, 2003

"We live in an age that is driven by information. Technological breakthroughs…are changing the face of war and how we prepare for war."

—William Perry, Secretary of Defense

Information technologies have changed the way we live, work, shop, communicate, and even fight. Our dependence on information technologies have left us vulnerable to information warfare attacks.

Information Warfare can cover a broad spectrum and means something different depending on the perspective. To the Department of Defense it means a modification in warfighting techniques. For technically sophisticated computer experts it means hacking into protected computers, often at random, for personal amusement or gratification, and not necessarily with malicious intent. For those who support political or social movements it represents a leveling of the playing fields, permitting small numbers of cyber-warriors to control propaganda and gain support. For terrorists, it could represent the most powerful weapon.

When we talk about information warfare, we are talking about information systems used to cripple a government and economy. A well-organized series of cyber attacks could send the target society into disorder.

Cooperation between military leaders, political forces, academics and industry from around the globe is essential to protecting the world's information infrastructure. Over the last 10 years, world-class security information security specialists, government authorities, intelligence agencies and media representatives have been meeting at **InfowarCon**, the source for the latest thinking in the critical area of information warfare and infrastructure security.

By participating in **InfowarCon**, you'll have access to information that you cannot find anywhere else, including combating cyber attacks and the latest intelligence on counterterrorism and homeland security.

The risks are real—so are the solutions. Be sure you have every advantage in this critical fight—register for InfowarCon today.

Why you should attend:

- Evaluate the latest tactics for detecting and protecting against cyber attacks
- Examine emerging threats, targeting and tactics
- Discover what's new and on the horizon of cyberwar tools and technologies
- Better understand the economic impact of cyberterrorism
- Explore Fourth Generation Warfare
- Discuss the newest initiatives in Homeland Security
- Interact with the world's leading experts and network with your peers

Table of Contents

InfowarCon™

TRACK 1: NON-LETHAL TECHNOLOGIES

Chairman: Pierce Reed, Futurist, Advanced Programs, General Dynamics Armament and Technical Products

From the battlefields of Iraq to the streets of New York and L.A., a new range of technologies designed to immobilize an adversary are gaining momentum. This new and fascinating addition to InfowarCon will cover the full gamut of applications and technology for law enforcement and the warrior.

TRACK 2: HOMELAND DEFENSE

Chairman: Homeland Security Council, White House

9-11 changed not only how we live as citizens, but gave our government a new focus—and the result was the birth of the Department of Homeland Security. This entity brings myriad government agencies under its wing. These sessions will cover what we are doing and what we can do better.

TRACK 3: TECHNICAL

Lt. Colonel Daniel Ragsdale, Ph.D., Director I.T. and Operations Center, U.S. Military Academy Westpoint

The bits and bytes for geeks and non-geeks alike. Take a look at what's new and on the horizon of cyberwar tools and technologies.

TRACK 4: FOURTH GENERATION WARFARE

Chairman: Col. G.I. Wilson (Ret) USMC, Consultants, M2 Technologies

Fourth Generation Warfare includes all forms of conflict where the other side refuses to stand up and fight fair. What distinguishes 4GW from earlier generations is that typically at least one side is something other than a military force organized and operating under the control of a national government, and one that often transcends national boundaries.

TRACK 5: STRATEGIC COMMUNICATIONS, PERCEPTION MANAGEMENT AND MILITARY TRANSFORMATION IN OPERATION IRAQI FREEDOM

Chairman: Douglas H. Dearth, Co-Chair, InfowarCon 2003

This track will examine: key issues, trends, prospects and controversies associated with Strategic Communications and other Perception Management programs within the overall context of Information Operations, the ongoing military transformation and the War on Terrorism. Presenters and commentators will include American and British experts and thinkers in these fields. These sessions will be of particular interest to government officials, military personnel, academicians, news media practitioners and analysts, as well as any others interested in these challenging and dynamic issues.

TRACK 6: INFRAGARD: CYBERCRIME TO CYBERDEFENSE

Chairman: David Strothcamp C.P.A. C.I.S.A., Information Security Audit Manager; Cleveland Clinic Health Systems, Director Northern Ohio Chapter of InfraGard, Past Member of National InfraGard Executive Board

In its second year at InfowarCon, InfraGard will emphasize the successes of the private-public partnership so necessary to successful infrastructure defense. The goal of InfraGard is to enable the flow of information so that the owners and operators of infrastructure assets can better protect themselves, and thereby help the United States government better discharge its law enforcement and national security responsibilities

TRACK 7: SECURITY CONCEPTS AND MODELS FOR MANAGEMENT

High level views of cyberspace are necessary to design and implement policy. These sessions are designed to help professional and governmental managers look at solutions under the following different "microscopes": Pictures, the Wild West, Telecommunications and Effective Leadership.

TRACK 8: THURSDAY ONLY: SPECIAL AIR FORCE INFORMATION WARFARE CENTER AND AIR FORCE BATTLE LAB SESSION

Come see why the U.S. Air Force is at the forefront of new technologies—and why it is one of most elite and visionary military branches.

TRCCon 2003

Annual Counterterrorism & Homeland Security Conference & Expo

TRACK 1: PRIMARY TRACK—

Terrorism Intelligence Analysis and Counterterrorism Operations, Chem Bio Threats and Response, Insights on the War on Terrorism and Homeland Security Risk Management

TRACK 2: INNOVATIONS TRACK—

Terrorism Indications and Project Responder Knowledge Base

The Chief of Police for a major metro transit authority described the Terrorism Research Center's training and briefing sessions as "the best training I have ever received. Period."

To register for InfowarCon or TRCcon today, visit www.infowarcon.com or www.trccon.com.

UAV Helicopters

See an eye-catching array of unmanned Air Vehicles (UAV) from a full-sized model to versions that will fit in one hand. The display will be in front of the National Security Summit Exhibit area at the Washington Convention Center (across the street from InfowarCon and TRCcon 2003).

LIVE! CyberWar Games

Led by: White Wolf Consulting

Brought back by demand, you can learn what the hackers know by becoming one at InfowarCon's CyberWar Games! This exciting real-time exercise will take place throughout the two-day conference and is FREE to all attendees. Plus, there will be pre- and post-conference war game instruction available only to those who register for optional tutorials.

The War Room

Hosting a series of servers, routers, firewalls and networking gear, the War Room will be open to pre- and post-tutorial attendees on September 30 and October 3. It will be open to all conference attendees 24/7, beginning at 8:00 a.m. on October 1.

Here's How it Works:

Four classes of servers will be set up for the sole purpose of testing your network attack and computer presentation skills.

A variety of operating systems and configurations, ranging from easy to extremely difficult to crack, will be at your disposal (available locally to attendees and remotely via VPN). You pick the level of protection you want to test yourself against.

- **A technical team will be on hand to give you hints and tips, and to help you round out your skills**
- **You'll get firsthand experience identifying system weaknesses and penetrating your target**
- **War game rules will be available on-site**

Become a Remote Cyber-Warrior

Can't attend the conference? You can still play Cyber War Games!

- **Become a remote cyber-warrior and put your hacker smarts to the test without leaving your office or classroom**
- **Play individually or form teams at your school or organization**
- **Ideal for class exercises, corporate training or hands-on government experience**

We'll supply the software that lets you play, and the rest is up to you!

InfowarCon™

Tuesday, September 30, 2003

8:00am	REGISTRATION & COFFEE			
9:00am–5:00pm	T1: From C2W to NCW…and Beyond	T2: Countering the Dangerous IT Insider	T3: Hacking 101— Tools and Techniques	T4: CyberWar Games: Computer Network Attacks

Wednesday, October 1, 2003

7:45am	Welcome to InfowarCon and TRCcon			
8:00am–9:30am	Opening Addresses—From the Top Down: The Executive Branch of Government and CIP; Homeland Defense and Cyberterrorism: A Legislative View			
9:30am	P1. TRC PLENARY: Kill With a Borrowed Sword: Terrorism, Technology and Critical Infrastructure Protection			
10:00am	BREAK			
10:30am	P2: Why Non-Lethals Are Critical To Modern Combat			
11:00am	P3: The Commercial Satellite Imagery Revolution			
11:30am	P4: An Introduction to Fourth Generation Warfare (4GW) and Its Relation to the Information Age			
12:00 noon–1:30pm	LUNCH			
	Track 1	**Track 2**	**Track 3**	**Track 4**
1:30pm–3:00pm	1A: Policy and TRADOC	2A: Working with High Resolution Commercial Satellite Imagery	3A: Virtual Networks for Operations, Research, and IA Training, and Education	4A: Four Generations of Modern Warfare/Part I
3:30pm–5:00pm	1B: State of Non-Lethal Technologies	2B: Rating the States for Electric Energy Infrastructure Security	3B: HERF, EMP, and All That Jazz!	The Moral Imperative in 4GW/Part II 4B: Fourth Generation Judo

Thursday, October 2, 2003

8:15am	Greetings and Administrivia: Douglas H. Dearth, Conference Co-Chair, InfowarCon 2003			
8:30am	Opening Address: United States Secret Service Role in Homeland Security, Ralph Basham, Director, United States Secret Service			
9:00am	Keynote: IO in Operation Iraqi Freedom and the Global War on Terrorism			
9:30am	P5: The Private Sector, Academia and the Implementation of the National Strategy to Secure Cyberspace			
10:00am	BREAK			
10:30am	P6: War 2040			
11:00am	P7: IW and Hacktivism			
11:30am	P8: Applying Lessons Learned in Holistic Perimeter Protection to Critical Infrastructure Protection			
12:00 noon–1:30pm	LUNCH			
	Track 1	**Track 2**	**Track 3**	**Track 4**
1:30pm–3:00pm	1D: Non-Lethals—An Operator's Perspective	2D: Defending the Gold— Case Studies From the Olympics	3D: The Value of Honeypots	4D: Living With Terrorism for Thirty Years; Reflections From Experience
3:30pm–5:00pm	1E: Issues Surrounding Human Effects	2E: Meet the Weakest Link (Part One) From Wyatt Earp to Cyber Cop (Part Two)	3E: Spam Tracking and Covert Channels (Part One); Virtual Information Wars: The Perils of Automated, Distributed, and Coordinated Attacks (Part Two)	4E: When the Hurlyburly's Done

Friday, October 3, 2003

8:30am	REGISTRATION & COFFEE			
9:00am–5:00pm	T7: The Reality Gap: Which Threats are Defended Against, Which are Not?	T8: The Law of Cyberwar and Counterterrorism	T9: Computer Network Attacks Analysis	T10: Common Criteria for Information Technology Security Evaluation

Conference At A Glance

T5: Introduction to Computer Forensics	T6: Comprehensive Community Preparedness		

Track 5	Track 6	Track 7	Track 8
5A: Strategic Communications in the Bush Administration	6A: Information Security and Privacy In the Age of Terrorism	7A: The Economics of Infowar and CyberTerrorism	
5B: IO, Transformation & Counter-Transformation	6B: Practical Computer Forensics Techniques	7B: Operationalizing Information Risk Management (Part One) Protecting Public Safety Communications through Wireless Network Interoperability (Part Two)	

Track 5	Track 6	Track 7	Track 8
5D: The Media & the Military in Operation Iraqi Freedom	6D: Latest Protections of Trade Secrets and Intellectual Property	7D: Privacy vs Security Debate	8A: United States Air Force Information Warfare Battlelab
5E: Future Trends in Information Operations, Perception Management & Military Transformation	6E: Department of Homeland, Security FBI and InfraGard	7E: Understanding the Big Picture: Correlating and Visualizing Security Data	8B: Air Force Information Warfare Center

T11: Cross-Domain Solutions—Information Assurance that Protects, Secures and Filters			

TRCon 2003

Annual Counterterrorism & Homeland Security Conference & Expo

TRCcon October 1, 2003

7:45am	Please refer to InfowarCon Schedule
1:30pm	T1A: Mirror Image Redux: Understanding the Terrorist Mindset (Part One)
	BREAK
3:30pm	Mirror Image Redux: Understanding the Terrorist Mindset (Part Two)

TRCcon October 2, 2003

8:00am–10:00am	KEYNOTE: Al Qaeda 2005
10:30am–12:00pm	TP1: PLENARY: Suicide Bombers and Suicide Attacks
LUNCH	12:00PM–1:30PM
1:30pm–3:00pm	T1B: PT: Insights from the Front Lines on the War on Terrorism
	T2B: IT: Submit Your Idea!
	BREAK
3:30pm–5:00pm	T1C: PT: Terrorism Intel Analysis & Counterterrorism Ops
	T2C: IT: Terrorism Indications and Warnings

TRCcon October 3, 2003

8:00am–8:30am	KEYNOTE: Homeland Security 2005
8:30am–9:30am	TP2 PLENARY: Fourth Generation Warfare: Implications for Law Enforcement and Homeland Security
9:30am–11:30am	TP3: PLENARY: From Munich to Manhattan: Thirty Years of Counterterrorism Lessons Learned
LUNCH	12:00PM–1:30PM
1:30pm–3:00pm	T1D: Chem/Bio Threats and Response Panel
	T2D: IT: Project Responder Knowledge Base
	BREAK
3:30pm–5:00pm	T1E: PT: Homeland Security Risk Management: Insights from Industry
	T2E: IT: Holistic Interoperability: An Integrated Response to Chemical/Biological Attacks

InfowarCon Tutorials

8:00AM REGISTRATION & COFFEE

9:00AM–5:00PM

T1: From C2W to NCW…and Beyond

Dr. Dan Kuehl, Professor of Systems Security Concepts and Models for Management, Information Operations and Technology Department National Defense University, Washington, D.C.

This tutorial features some of the DOD's leading experts from the National Defense University, who will bring you up-to-date on the "state of the field" in Information Operations. We'll look at developments in Information Assurance/Critical Infrastructure Protection and their contributions to Homeland Security. We'll examine the doctrinal and operational developments in IW/IO, especially as influenced by the War in Iraq and also how we are using Information Power to shape and influence attitudes globally.

T2: Countering the Dangerous IT Insider

Jerrold M. Post, M.D., President, Political Psychology Associates, Ltd.

This tutorial systematically addresses the identification and Security Concepts and Models for Management of the dangerous information technology insider problem. It reviews perpetrator psychological characteristics, develops a typology of perpetrators, and reviews the way in which dysfunctional Security Concepts and Models for Management can contribute to employee disloyalty. Case material will be utilized throughout.

T3: Hacking 101—Tools and Techniques

Eric Naylor, Ph.D. White Wolf Consulting

In this ever-popular tutorial you will explore the latest hacking tools and techniques and learn the step-by-step methodology behind hacking. You will learn target reconnaissance, vulnerability mapping, port scanning, password cracking, Trojan horse programs and Denial of Service attacks along with countermeasures for thwarting them. Demo computers and scatter attack/defend laptops will let you view countermeasures in action. Bring your laptop "armed" with wireless (80211.b) PCMIA already installed.

T4: CyberWar Games: Computer Network Attacks

Tim Rosenberg, Esq., Ron Plesco, Esq., White Wolf Consulting, Brian D. Best, Cisco Optical Specialist 1/Systems Engineer

This advanced one-day tutorial will launch the opening salvo of three intensive days of computer cyber war games. Using your own wireless laptop and provided VPN software, you will walk through a series of "hands-on, hands-off" sessions employing the latest network reconnaissance and attack tools against a "victim" server farm, and more.

T5: Introduction to Computer Forensics

Warren G. Kruse II, CISSP, CFCE Computer Forensic Services, LLC

This tutorial will give you a good solid overview and many tools to introduce you to forensics. Learn the basics of computer forensics, build your Digital Forensics Toolkit, discover proven investigative strategies and learn proper evidence handling procedures. The day will include Windows and Unix forensics.

T6: Comprehensive Community Preparedness

Greg Moser, Plans, Training and Exercises Coordinator, Jefferson County (Colorado) Office of Emergency Security Concepts and Models for Management

This INTENSIVE PREPAREDNESS tutorial is your opportunity to learn how to build a safer, more resilient and more responsive community. Homeland Security requires a practical, sustainable, integrated and comprehensive program for dealing with all the hazards that threaten our communities. This tutorial will give you the information, tools and procedures to build the program that is right for your community.

InfowarCon Sessions

Wednesday, October 1, 2003

7:45AM

Welcome to InfowarCon

Winn Schwartau, Founder, InfowarCon™, InfowarCon.com; Douglas H. Dearth, Co-Chair, InfowarCon 2003

8:00AM–9:30AM OPENING ADDRESSES

From the Top Down: The Executive Branch of the Government and CIP

Paul B. Kurtz, Special Assistant to the President and Senior Director for Critical Infrastructure Protection, The White House;

Vice Admiral Lowell E. Jacoby, USN, Director, Defense Intelligence Agency

Homeland Defense and Cyberterrorism: A Legislative View

Congressman Jim Turner (TX-D), Ranking Member, Committee on Homeland Security

9:30AM

P1: TRC PLENARY: Kill With a Borrowed Sword: Terrorism, Technology and Critical Infrastructure Protection

Matthew G. Devost, President and CEO, Terrorism Research Center, Inc.

Modern societies are inherently reliant on exploitable technologies and public perceptions to ensure the successful operation of our critical infrastructures. This session provides a quick overview of how terrorists have "weaponized" these elements of our society against us in the past and provides insights into what elements may be attacked or exploited in the future.

10:00AM BREAK

10:30AM

P2: Why Non-Lethals Are Critical To Modern Combat

Marshall "Will" Williams, USARMY Command; Sgt. Major, (Ret) Director of Government Relations, General Dynamics

"Will" Williams was a career Special Operations soldier in the United States Army prior to his retirement as a Command Sgt. Major and senior enlisted Advisor to the Secretary of Defense in 2002. Will is a combat-experienced NCO and participated in several urban operations including high-visibility actions in Panama and Somalia. Today, Will works in government relations for the defense industry and is active in advocating the development and rapid deployment of non-lethal technologies.

11:00AM

P3: The Commercial Satellite Imagery Revolution

John Pike, Director, GlobalSecurity.org

John Pike, the leading pioneer of innovative applications of commercial satellite imagery, discusses how this imagery is transforming a diverse range of knowledge domains, including electronic news gathering, proliferation of weapons of mass destruction, regional military intelligence collection and humanitarian relief.

11:30AM

P4: An Introduction to Fourth Generation Warfare (4GW) and Its Relation to the Information Age

Rick Forno, Security Consultant and Author

This session provides an reality-based overview of the concept of Fourth Generation Warfare (4GW) and then examines how, in today's world, 4GW can become an effective technique by state and non-state actors during both wartime and peacetime.

12:00 NOON–1:30PM LUNCH

1:30PM–5:00PM BREAKOUT SESSIONS

TRACK 1: NON-LETHALS

Track Chair and Moderator: R. Pierce Reid, Futurist, Advanced Programs General Dynamics Armament and Technical Products

1:30PM–3:00PM

1A: Policy and TRADOC

Panel: Bancroft McKittrick, & COL, GI Wilson (Ret) USMC, Consultants, M2 Technologies; Matt Begert, Project Leader, National Law Enforcement & Corrections Technology Center—West; Col. John Alexander (Ret), Consultant and Author of "Future War"

This session will explore the important issues surrounding usage policy for non-lethals as well as the training and doctrine associated with the deployment and employment. Because use of lethal force has been accepted for millennia, the policies and even liabilities associated with its use are well-defined and well-understood. For less-than-lethal technologies, the policies are neither defined nor well-understood and the doctrine has yet to be created and codified. This track will explore the issues surrounding the creation of policy, doctrine and training for the deployment of tomorrow's non-lethal technology.

3:30PM–5:00PM

1B: State of Non-Lethal Technologies

Panel: John Cline, Systems Manager for Non-Lethal, Combat Tech and Concepts Team, Picatinny Arsenal, USARMY ARDEC; Dr. John Kinney, Institute for Non-Lethal Defense Technologies at Penn State University; Peter Woodson, Manager, Advanced Programs/ Non-Lethal, General Dynamics Armament and Technical Products

In the past few years, there has been a surge in research and development of non-lethal technologies ranging from Malodorants to Capcaisin. This panel will explore the state of today's non-lethal technologies and will discuss capabilities that are on the near horizon, demonstrating that today's science fiction will be tomorrow's science fact.

TRACK 2: HOMELAND DEFENSE

1:30PM–3:00PM

2A: Working with High Resolution Commercial Satellite Imagery

John Pike, Director, Global Security.Org

This session will examine practical strengths and limitations of this new information resource. Based on his unique first-hand experience in working with commercial imagery and other open source intelligence resources, Mr. Pike shares some hard-won insights into this extremely challenging yet highly rewarding resource.

3:30PM–5:00PM

2B: Rating the States for Electric Energy Infrastructure Security

Joel Gordes, Environmental Energy Solutions

This session will address vulnerabilities at the state level that are built into energy systems. Central to this discussion will be a prototype checklist that can be used to identify how vulnerable each state might be to both physical and cyberattacks against their critical energy infrastructure.

TRACK 3: TECHNICAL

1:30PM–3:00PM

3A: Virtual Networks for Operations, Research, and IA Training, and Education

Lt. Colonel Daniel Ragsdale, Ph.D., Director I.T. and Operations Center, U.S. Military Academy Westpoint; Major Ronald Dodge, Ph.D., Cadet Shaun Baker USMA, Westpoint

An ongoing initiative at the United States Military Academy (USMA), the Virtual Information Assurance Network (VIAN) provides a robust and fully configurable virtual network that requires only one single workstation. It can be configured to provide intrusion detection, early warning, and network deception, and is also useful for data collection in support of IA research.

3:30PM–5:00PM

3B: HERF, EMP, and All That Jazz!

Rostislav Persion, SUNY, New York

This session will cover threats of homemade electromagnetic weapons on our infrastructure. HERF, EMP and EMI devices, which can be of great threat, can easily be constructed with today's technology available to most consumers. Rostislav will demonstrate a few miniature-scale homemade EMI/EMP devices and will explain their operation, construction and effective preventative measures against small-scale EMI/EMP attacks.

TRACK 4: FOURTH GENERATION WARFARE

1:30PM–3:00PM

4A: Four Generations of Modern Warfare/Part I

Speaker: William S. Lind, Free Congress Foundation; Track Chair: COL. G.I. Wilson, (Ret) USMC, Consultant, M2 Technologies Moderator: Rick Forno Security Consultant and Author

This session will lay out the framework of the Four Generations of Modern War—War from the Peace of Westphalia in 1648, which gave the state a monopoly on war through French (and American) firepower/attrition warfare and German maneuver warfare to emerging Fourth Generation Warfare, where the state loses.

The Moral Imperative in 4GW/Part II

Gregory Wilcox, Senior Systems Analyst, Manager, Engineering Systems Division, SRI International

John Boyd identified three aspects of war: physical, mental and moral. Clearly America does well in the physical and mental aspects of war as were so recently proved in Iraq. It is the moral aspect of war, and particularly 4GW that we fail to fully understand. Our 4GW enemies are willing to die for their cause, which is for fundamental religious purposes. The suicide bombers, including September 11th, have been extremely effective in creating terror and panic in the communities that they have attacked. In this session, we will look for the root issues and causes and begin to seize the moral high ground.

3:30PM–5:00PM

4B: Fourth Generation Judo

COL. G.I. Wilson, (Ret) USMC Consultant, M2 Technologies

As the technological way of warfare evolves, our foes are embracing Fourth Generation Warfare (4GW) as a modus operandi. Nation states no longer hold a monopoly on violence. Too often our military rely solely on technological solutions to warfare rather than operational solutions. A mistake our enemies are betting we will continue to make using fourth generation judo to leverage our overreliance on technology against us.

TRACK 5: STRATEGIC COMMUNICATIONS, PERCEPTION MANAGEMENT & MILITARY TRANSFORMATION IN OPERATION IRAQI FREEDOM

Track Chair: Douglas H. Dearth, Conference Co-Chair

1:30PM–3:00PM

5A: Strategic Communications in the Bush Administration

LCDR Leigh Armistead, U.S. Navy
Comments by Professor Phil Taylor, University of Leeds, UK

It has long been understood that effective Strategic Communications and Public Diplomacy are central tools in a nation's Strategic Communications, Perception Management campaign. For the United States, these requirements have only gained heightened importance in support of the global War on Terrorism. LCDR Leigh Armistead will present an analysis of the record of the Bush Administration in formulating and operationalizing an effective Strategic Communications program in pursuit of its foreign policy goals. Further commentary on the issues will be provided by British media expert, Professor Phil Taylor.

3:30PM–5:00PM

5B: IO, Transformation & Counter-Transformation

Dr. Michael E. Vlahos, Johns-Hopkins University Applied Physics Lab; Commentators: Professor Dan Kuehl, National Defense University; Mr. Charles A. Williamson, Department of Defense

This session will examine the main features of the ongoing Military Transformation, as well as certain trends that might inhibit or retard its full accomplishment. The key issues presented and examined by strategist Dr. Mike Vlahos of Johns Hopkins University will be critiqued from academic and government perspectives by long-time conference contributors Professor Dan Kuehl from the National Defense University and by Mr. Chuck Williamson of the Department of Defense.

TRACK 6: INFRAGARD: CYBERCRIME TO CYBERDEFENSE

1:30PM–3:00PM

6A: Information Security and Privacy In the Age of Terrorism

Mark D. Rasch , Esq. Senior Vice President and Chief Security Counsel, Solutionary Inc.

This session will cover Federal Privacy and Security Legislation and Regulations since 9-11. Effects of Gramm-Leach-Bliley Act Title V, Patriot Act of 2001, Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act and HIPAA Regulations upon our personal rights to security and personal privacy.

3:30PM–5:00PM

6B: Practical Computer Forensics Techniques

Kristopher Sharrar, CISSP , Lead Forensic Consulting Manager James Halley, Computer Forensic Manager Ernst & Young L. P. Cleveland National Office

A "Case Study" approach detailing "lessons learned" in real cases. In the second half of this session, we'll discuss the practical and technical aspects of a representative sample of the most challenging cases we've worked on. To protect certain sensitivities, we've changed the names of companies, their industries, their products and other data, however the challenges faced will be accurately described.

TRACK 7: SECURITY CONCEPTS AND MODELS FOR MANAGEMENT

1:30PM–3:00PM

7A: The Economics of Infowar and CyberTerrorism

Scott Borg, Research Fellow, Tuck School of Business at Dartmouth

How much does cyberwar cost an economy? What are the economic ramifications on societal productivity if significant components of our CIs are disrupted? What about the costs to businesses and stock markets when information is altered or suddenly made public?

These are the questions that have been loosely asked but never formally studied. Mr. Borg will provide the answers as they have never been provided before: a formal mathematical approach to evaluating the economic impact of Cyberterrorism.

3:30PM–5:00PM

7B: Operationalizing Information Risk Management (Part One)

Rolf Moulton, CISSP, CISA, CCP, Risk Reduction Solutions (Presenter); Robert S. Coles, MBA, MBCS, CISM (Coauthor) Partner Service Leader, Information Security Services. KPMG LLP London, England

This session will help you make sure that you and the "risk takers" in your organization agree on which information risks need to be managed. Focus will be on prioritizing what will be protected, what needs to be done, alternative approaches to do the job and how to keep the whole team playing the same game.

Protecting Public Safety Communications Through Wireless Network Interoperability (Part Two)

Scott Forbes, Nextel Communications

Much of the emergency response capabilities of America's public safety agencies, such as local fire departments, the Department of Justice and the National Guard, hinge on effective and immediate interoperable wireless communications across geographic and jurisdictional boundaries. This presentation will discuss these limitations and offer practical solutions that promote secure and interoperable wireless public safety communications.

8:15AM

Greetings and Administrivia

Douglas H. Dearth, Conference Chair

8:30AM–9:30AM OPENING ADDRESSES

8:30AM

The United States Secret Service Role in Homeland Security

Ralph Basham, Director, United States Secret Service

9:00AM

Keynote Address: IO in Operation Iraqi Freedom and the Global War on Terrorism

Brig. Gen. Jack J. Catton Deputy Director for Information Operations, Joint Staff

Since September 11, 2001, IO in all its aspects has played a central role in the global War on Terrorism. In Operation Iraqi Freedom, IO also played a key role, from the perception management campaign before and during the combat phase, to precision-targeting in combat, to protecting U.S. and Allied forces' command-and-control infrastructure. This presentation by the officer responsible for IO on the Joint Staff will outline the nature of these IO efforts, including the challenges associated with them.

9:30AM

P5: The Private Sector, Academia and the Implementation of the National Strategy to Secure Cyberspace

Dr. Phyllis A. Schneck, Vice President, Enterprise Services, eCommSecurity, Inc. Chairman, National Executive Board, FBI InfraGard

After months of input and advice-gathering from public and private companies of all sizes as well as Universities around the Nation, the President's Critical Infrastructure Protection Board issued the final version in late 2002 of our National Strategy to Secure CyberSpace, while a new Department of Homeland Security was being created. Now that all are functional, we have the tools needed to centralize information sharing to secure our infrastructures and our country. How can we best use the strategy as a road map? Where do we start? This discussion will feature a long Q&A session to address these issues directly from the perspective of the audience.

10:00AM BREAK

10:30AM

P6: War 2040

Winn Schwartau, Founder, InfowarCon
The Security Awareness Company

Winn helped redefine the concept of war in the late '80s and early '90s, often to intense public derision. In the last year, he was asked to look forward almost 40 years and tell us what he sees. What will warfare be like? Who will be the actors? What technologies will be used? What lessons can we apply to the security of the future? Find out here.

11:00AM

P7: IW and Hacktivism

Dr. Dorothy E. Denning, Dept of Defense Analysis, Naval Postgraduate School

Recent years have seen an increase in self-appointed cyber warriors hacking for human rights and attacking the computer networks of those they condemn. They have surfaced in conflicts worldwide, particularly those relating to the Middle East, China, Kosovo, Mexico, India, Pakistan and the United States. This talk will review the state of hacktivism worldwide as well as trends.

11:30AM

P8: Applying Lessons Learned in Holistic Perimeter Protection to Critical Infrastructure Protection

Gene Fredriksen, VP Information Security, Raymond James and Associates

When a task seems too large and complex to handle, it is time to review the basics and break the larger task into manageable sub-tasks. That is certainly the case with today's critical infrastructure protection issues. We will look at the basic components of developing a holistic perimeter protection plan and applying it to the larger tasks of infrastructure protection.

12:00 NOON–1:30PM LUNCH

1:30PM–5:00PM BREAKOUT SESSIONS

TRACK 1: NON-LETHALS

Track Chair and Moderator: R. Pierce Reid, Futurist, Advanced Programs General Dynamics Armament and Technical Products

1:30PM–3:00PM

1D: Non-Lethals—An Operator's Perspective

Panel: Jeff Hoke, Marine Corps Representative to the DoD Joint Non-Lethal Development Task Force Members of the Seattle SWAT and Lethal Cadre Leader, Tim Pasternak; Bruce Emerson, Law Enforcement Expert, Non-Lethals

This session will explore the user perspective on the situations warfighters and police officers encounter in the streets and on the battlefields. The military perspective will include lessons learned in Afghanistan and Iraq and in law enforcement. Users will have perspective from combat; from crowd control and domestic riot situations; "suicide by cop" perspective; and experience in rural and resort law enforcement.

3:30PM–5:00PM

1E: Issues Surrounding Human Effects

Dr. Glenn Shwaery, Director, University of New Hampshire's Non-Lethal Technology Innovation Center; Joseph Rutigliano, Attorney-Advisor, International and Operational Law Branch SJA to CMC, Headquarters, U.S. Marine Corps

One of the biggest challenges for the deployment of non-lethals will be the exploration of human effects. The liability issues surrounding the use of non-lethals must be addressed by human effects testing to avoid the possibility of unintended effects ranging from eye damage to death from agents that were intended to be non-lethal. This panel will explore the challenges of effects testing and the current state of the art in this critical area.

TRACK 2: HOMELAND DEFENSE

1:30PM–3:00PM

2D: Defending the Gold—Case Studies From the Olympics

Leia Amidon CISSP, Partner/Principal Security, Technologist, SunStorm Security Group

In this session, we will step through real-world bastion architecture design and analyze actual fortress defense strategies and tactics, including the 2002 Olympic Games, stock exchanges, military command centers and regional critical infrastructure. There will be three interactive sessions, in which you will assess the risk profile of a target, learn to recognize anomalous traffic patterns, and participate in a war-room response exercise.

3:30PM–5:00PM

2E: Meet the Weakest Link (Part One)

Lloyd Reese, CISSP, CPP Former Sr. InfoSec Specialist, Dept. of Veteran's Affairs

Most approaches to enterprise risk management are limited to information security with an occasional mention of physical security and business continuity planning. The weakest link in the chain is the one most likely to fail, yet, may not be included in the traditional approach. This link may be outside the organization as a part of the external infrastructure: water, power, telecommunications or even key suppliers.

From Wyatt Earp to Cyber Cop (Part Two)

Arthur C. Jones, Doctorial Student, University of PA

As incidents of cyber crime become increasingly common, a look at individuals and organizations that comprise the criminal justice system as it relates to "traditional crime," past and present, may reveal methods for combating this threat. This session will review the various functions of the law enforcement community, both official and unofficial, and seeks to identify appropriate equivalents or substitutions in the realm of computer-based crime environment.

TRACK 3: TECHNICAL

1:30PM–3:00PM

3D: The Value of Honeypots

Lance Spitnzer, Senior Security Architect, Sun Microsystems and Founder of the Honeynet Project

Honeypots are an emerging technology with incredible potential for the security community. They help address the problems of many existing technologies, including detection and information-gathering. In this exciting presentation, Lance Spitzner will cover what honeypots are, their value and examples of how they can (and have been) used.

3:30PM–5:00PM

3E: Spam Tracking and Covert Channels (Part One)

Dr. Neal Krawetz, Hackerfactor.com

This session covers methods for identifying forged emails and tracking individual senders. Categories are provided for classifying spam by function, including List Makers, Scams and Covert Communication channels. It will contain case studies, including how to use spam as a covert communication channel, which is especially critical in a world where the good and the bad use the same broadcast infrastructure.

Virtual Information Wars: The Perils of Automated, Distributed, and Coordinated Attacks (Part Two)

Dr. Sviatoslav Braynov, Assistant Professor, Dept. of Computer Science and Engineering SUNY, Buffalo

This session will present research results and ideas in the area of virtual information wars. We will demonstrate current attack patterns that have not utilized the full potential for real-time coordination and cooperation between intelligent software agents such as softbots and robots, etc.

TRACK 4: 4TH GENERATION WARFARE

1:30PM–3:00PM

4D: Living With Terrorism for Thirty Years; Reflections From Experience

Victor O'Reilly, Author

Combating terrorism in a Fourth Generation Warfare setting requires brainpower ahead of firepower—though both are needed. A purely physical force reaction to terrorists tends to be disastrous. Counterterrorism in 4GW context requires patience, stamina, resolve and, above all, intelligence—in every sense of the word. Technology can be helpful, too, but it runs a far and distant second to the human dimension.

3:30PM–5:00PM

4E: When the Hurlyburly's Done

Franklin C. Spinney, Retired Analyst, Pentagon, Office of Program Analysis and Evaluation in the Office of the Secretary of Defense

The preemptive assault on Iraq has generated enormous grand strategic repercussions, particularly among our traditional allies, which are still playing out in an unknowable directions. 4GW warriors, like Osama bin Laden, aim to bypass traditional military structures and attack directly at political, economic and cultural sources of power. They want us to lash back with a brutal unfocused retaliation, especially against innocents, because that will give them grand-strategic leverage.

TRACK 5: STRATEGIC COMMUNICATIONS, PERCEPTION MANAGEMENT & MILITARY TRANSFORMATION IN OPERATION IRAQI FREEDOM

1:30PM–3:00PM

5D: The Media & the Military in Operation Iraqi Freedom

Professor Phil Taylor, University of Leeds, UK
Commentators: Mr. Michael Marriott Marriott Video Productions

This session also will include journalists who accompanied Allied military forces in Operation Iraqi Freedom.

Recent operations in Iraq have reignited long-standing controversies surrounding the wartime relationship between Allied military forces and the international news media. Does a close working relationship essentially make the media part of the military propaganda effort? This session will examine in detail the evolving nature of the media-military relationship and future prospects for the policy of "embedding" journalists in Allied military units. British military-media expert, Professor Phil Taylor, along with veteran Australian combat journalist, Mike Marriott, covered the war in Iraq and will analyze these issues.

3:30PM–5:00PM

5E: Future Trends in Information Operations, Perception Management & Military Transformation

D.H. Dearth, Conference Co-Chair; Commentators: Professor Phil Taylor, University of Leeds, UK; Dr. Michael Vlahos, Johns-Hopkins University; Professor Dan Kuehl, National Defense University, LCDR Leigh Armistead, U.S. Navy

Based upon the foregoing three Track discussions, this session will attempt to draw out key future trends and prospects for Perception Management programs, highlighting their role and utility in overall Information Operations and the ongoing Military Transformation and War on Terrorism. Conference Co-Organizer, Doug Dearth, will posit a number of key themes and trends, with further commentary and critique by a panel of experts.

TRACK 6: INFRAGARD: CYBERCRIME TO CYBERDEFENSE

David Strothcamp, Chairman C.P.A. C.I.S.A., Information Security Audit Manager, Cleveland Clinic Health Systems, Director–Northern Ohio Chapter of InfraGard, Past Member of National InfraGard Executive Board

1:30PM–3:00PM

6D: Latest Protections of Trade Secrets and Intellectual Property

Dave Drab, Principal Intellectual Asset Security Concepts and Models for Management, Xerox Global Services, Inc.

Trade secrets are the lifeblood of competition and therefore an integral part of trade, commerce and industry. Companies victimized by economic espionage experience loss of competitive advantage, erosion of market share, reduction in revenue streams and the loss of shareholder confidence. Unfortunately, most companies do not properly identify, manage and protect their trade secrets, and in many cases, the crises that result could have been avoided. Xerox and its partners are developing solutions that will ultimately protect and enhance the value of all intellectual assets.

3:30PM–5:00PM

6E: Department of Homeland Security, FBI and InfraGard Success Stories from a Partnership Between Government and Private Sector Community

Dr. Phyllis Schneck and David Strothcamp

The NIPC has moved to the Department of Homeland Defense, but the InfraGard mission of coordinating public-private cooperation is key to successful cyber-defense. In conjunction with the FBI, this partnership has yielded successes and many lessons that can be applied to local and state organizations, including State Infrastructure Protection Centers.

TRACK 7: SECURITY CONCEPTS AND MODELS FOR MANAGEMENT

1:30PM–3:00PM

7D: Privacy vs Security Debate

Moderator: Rich Hale, Chief Information Assurance Executive, DISA; Panelists: Vincent Anthony, Former Homeland Security Director, CSC; Anthony Martini, DigiGAN, President, and several others

The issues of security and privacy are vital to information technology. We recognize the need to balance two opposing forces as information security initiatives advance: **1. Enablement or Inclusive**—Representing an imperative that the right people require controlled access to the right resources. **2. Protection or Exclusive**—an organization's information assets be protected to ensure integrity, privacy and reliability.

3:30PM–5:00PM

7E: Understanding the Big Picture: Correlating and Visualizing Security Data

Dr. Anita D'Amico, Director, Stephen J. Salas, Project Engineer, Secure Decisions

This session will review state-of-the-art technologies for collecting and analyzing security data from firewalls, IDSs and other sensors. You will see examples of how to identify suspicious insider activity by combining data from network and physical security sensors, and how to gain insight into the business impact of security incidents from your network data.

TRACK 8: AIR FORCE INFORMATION WARFARE CENTER & AIR FORCE BATTLE LAB

1:30PM–3:00PM

8A: United States Air Force Information Warfare Battlelab

Michael Jackowski , Technical Director, IW Battlelab

The Air Force Information Warfare Battlelab (AF-IWB) is one of seven Air Force Battlelab's charged to rapidly identify innovative Information Operation (IO) technologies, demonstrate its military worth and facilitate transition into today's combat Air Force. The AF-IWB works hand-in-hand with AF major commands, sister services, various government agencies, academia and industry to advance innovative ideas. The Battlelab's InfowarCon presentation will cover the process for evaluating, selecting and demonstrating innovative technologies, as well as several examples of demonstrated technologies that have already transitioned into the operational world.

3:30PM–5:00PM

8B: Air Force Information Warfare Center

Major Jeff Clay, Defensive Information Operations Technology Division

The Air Force Information Warfare Center (AFIWC) is one of four Air Force Warfighting Centers and is the only one that provides combatant commanders with information warfare (IW) capabilities to execute offensive and defensive counter-information missions. This session will comprise a threat overview, evolving changes in protecting AF enterprise systems and near-term/long-term challenges of the AF IW mission. The threat briefing will provide the session attendees with a good foundation for the following briefings on effective protection of AF enterprises and future challenges.

InfowarCon Tutorials

8:00AM REGISTRATION & COFFEE

9:00AM–5:00PM

T7: The Reality Gap: Which Threats are Defended Against, Which are Not?

Alan E. Brill, CISSP, CFE, Senior Managing Director, Technology Services, Kroll, Inc

Kroll, Inc. is often called on to investigate computer incidents in the corporate world. We have gained important insights into the real way that incidents occur, and why they will continue to occur. In this enlightening session, world-renowned expert Alan Brill looks at the gap that exists between assumptions made by many computer security professionals about what they need to do to defend their systems, and the ways that the attacks really materialize. It turns out that many vital elements of defense are not necessarily difficult, complicated, expensive or even high-tech. Learn how to close the reality gap in this interactive session.

T8: The Law of Cyberwar and Counterterrorism

Walter Gary Sharp, Sr., Director of Global and Functional Affairs/Bureau of Legislative Affairs U.S. Department of State

Cyberwar and terrorism challenge traditional U.S. domestic, international and foreign law paradigms. The legal authority for a state to respond to acts of cyberwar and terrorism is actor-dependent. For example, terrorists who are non-state actors are criminals and murderers who warrant a law enforcement response, and states that sponsor terrorism are led by despots who are subject to the lawful use of armed military force. This tutorial explores whether existing U.S. domestic, international and foreign law paradigms effectively preserve a state's inherent right of self-defense in the face cyberwar and terrorism. It will analyze in detail what international law applies to transnational terrorist networks and state sponsors of terrorism, how the law of conflict management and the law of war apply in a war against terrorism, what legal status applies to terrorists under the law of war, what fora are available to prosecute terrorists and the many legal consequences of declaring war on terrorism.

T9: Computer Network Attacks Analysis

Scott Zimmerman, CISSP, Independent Consultant

After three Cyberwar intense days of attacks and defend, the final tutorial will walk students through the basics CAN and CND of system and network forensics. You will learn how to utilize the logs from the Tuesday tutorial and the war games. We will demonstrate how to discover what has happened in our protected environment. You will cover a variety of tools and tips on how to handle victim servers for forensic analysis. Topics include log location and format, log analysis, IDS use and the basics of system analysis. Bring your wireless laptop, CD and burn a copy of the logs on the spot!

T10: Common Criteria for Information Technology Security Evaluation

Ms. Jean H. Schaffer, Director of the NIAP CCEVS Validation Body, (NIAP is a strong collaborative effort between NIST and the NSA)

The purpose of this tutorial is to familiarize participants with the International Common Criteria for Information Technology Security Evaluation (ISO 15408), usually known as the Common Criteria. Participants will be exposed to a high-level introduction of the CC standard; the current policies regarding Common Criteria testing; the role of evaluated products in government Information Technology acquisition, certification and accreditation; the process for CC product evaluation; the process for becoming a certified evaluation laboratory; and helpful hints for vendors who are interested in having their product evaluated. All participants would receive a copy of the CC Toolbox and the Common Criteria (on CDs). Participants should gain an understanding of the Common Criteria standard and understand the process for getting a product evaluated as a result of this tutorial.

T11: Cross-Domain Solutions— Information Assurance That Protects, Secures and Filters

Aaron Ferguson, Cross Domain Solutions Working Group, NSA; George Romas, CTO, CACI International; Dave Thompson, Developer, DigiGAN; Lt. Cmdr. Edward Bryant

Today's global environment is changing the nature of conflict and necessitating a fundamental shift in the demand for cross-domain technologies. A need has arisen to enact change across the intelligence and defense communities in order to best protect data, secure networks and filter traffic. In this tutorial you will discover how next-generation, cross-domain solutions are essential to enabling mission critical information-sharing between security domains to achieve cross-jurisdictional communication and collaboration. Learn about strategies for planning cross-domain solutions, the technologies available to support initiatives, and tactical implementations. This tutorial will include four sessions: **Strategy:** overview of the problem/current situation, current needs, future road map; **Technology:** presentation of the technologies currently implemented and their shortcomings; new and emerging technologies that will enable CDS; **Tactical:** a discussion of how the available technologies can be implemented; and **Case Study:** a working example of cross-domain solutions and a presentation of specific known needs. We will then move to a Conclusion with all panelists for concluding statements and Q&A.

Registration Information

Registration Desk Times

Tuesday: 7:30am–5:00pm; Wednesday: 7:15am–5:00pm; Thursday and Friday: 7:30am–5:00pm

Event Registration Options	Before 8/25/03	After 8/25/03 & Onsite
InfowarCon Conference *(Full InfowarCon conference on Wednesday and Thursday ONLY, does not include tutorials or TRCcon)*	$995	$1,195
TRCcon Conference *(Includes TRCcon conference and Wednesday morning plenary sessions ONLY, does not include InfowarCon conference or tutorials)*	$695	$795
InfowarCon & TRCcon Conference *(Full InfowarCon and TRCcon conference on Wednesday, Thursday and Friday)*	$1,495	$1,695
Two Tutorials *(Includes two tutorials on Tuesday and Friday ONLY, no InfowarCon or TRCcon Conference)*	$595	$695
One Tutorial *(Includes one tutorial on Tuesday or Friday ONLY, no InfowarCon or TRCcon Conference)*	$395	$495

For qualified Educational Groups, Military Educational Institutions, Group and InfraGard discounts, please call 727-360-4061.

To register visit www.infowarcon.com or www.trccon.com, or call 800-875-7556

All fees must be paid in U.S. dollars. Registration fee includes admission to sessions, all session materials (not including tutorials), refreshments, continental breakfasts, lunch on Wednesday and Thursday and receptions. Tutorial fee includes lunch, refreshments and materials for tutorials you attend.

Student Registration

Students currently registered in public, private or military institutions of higher learning can attend conferences at a discounted rate. Please call 727-360-4061.

Travel and Accomodations

InfowarCon 2003 and TRCcon convenes at the Renaissance Washington D.C. Hotel. Thanks to Sabre®, the #1 travel software provider in the world, we can offer you the lowest available rates for your hotel, airline and car rental. You can choose from an array of discounted hotel options. For details:

Visit: www.infowarcon.com or www.trccon.com

Call: 800-388-8108, 7:00am–6:00pm, Monday–Friday CST, or 312-527-7300

Fax: 312-329-9513

E-mail: infowarcon@ttgonline.com

InfowarCon™

TRCCon 2003

Annual Counterterrorism & Homeland Security Conference & Expo

TRCcon DAY ONE—OCTOBER 1, 2003

7:45AM–9:30AM

Please refer to InfowarCon Schedule

9:30AM

P1. TRC PLENARY: Kill With a Borrowed Sword: Terrorism, Technology and Critical Infrastructure Protection

Matthew G. Devost, President and CEO, Terrorism Research Center, Inc.

Modern societies are inherently reliant on exploitable technologies and public perceptions to ensure the successful operation of our critical infrastructures. This session provides a quick overview of how terrorists have "weaponized" these elements of our society against us in the past and provides insights into what elements may be attacked or exploited in the future.

10:30AM–12:00PM

P2, P3, P4, See InfowarCon Descriptions

12:00PM–1:30PM LUNCH

AFTERNOON SESSIONS

1:30PM–3:00PM

T1A: Mirror Image Redux: Understanding the Terrorist Mindset

Bryan Vossekuil, Dr. Robert Fein, With Special Guests

This session provides insight from historical and current analysis of terrorists and perpetrators of mass casualty violence to provide unique insight into the psychological factors of terrorism. In order to identify and respond to terrorists, we must have insight into their mindset, decision-making processing and unique external influences such as culture, training and religion.

3:00PM BREAK

3:30PM–5:00PM

Mirror Image Redux: Understanding the Terrorist Mindset (continued)

TRCcon DAY TWO—OCTOBER 2, 2003

8:00AM–10:00AM

KEYNOTE: AL QAEDA 2005

Brian Michael Jenkins, RAND Corporation

International terrorism expert Brian Michael Jenkins provides his insight into the emerging threats posed by Al Qaida and other global and domestic terrorist groups. He will provide an overview and assessment regarding the effectiveness of the "war on terrorism" and what measures will be required to address the global threat of terrorism.

10:30AM–12:00PM

TP1: PLENARY: Suicide Bombers and Suicide Attacks

Walter Purdy, Terrorism Research Center, Inc.
Col. Sami Barak, Former Counterterrorism Advisor to Israeli Prime Minister

Suicide bombings have emerged over time as one of the preferred and most effective mechanisms for terrorist attacks. This panel provides an analysis of suicide bombings with a focus on emerging suicide bombing threats and prevention tactics and includes presentations that have recently been noted as the best on the topic currently available.

12:00PM–1:30PM LUNCH

1:30PM–3:00PM

T1B: Primary Track: Insights from the Front Lines on the War on Terrorism

Col. Danny McKnight (US Army, ret.): commander of the ground convoy in the Black Hawk Down assault; Sebastian Junger: Best-selling author and international journalist; Robert Young Pelton: International traveler and author of "The World's Most Dangerous Places," "Come Back Alive" and others.

This panel provides firsthand insights and experience from the front lines of current and emerging terrorist hotspots. Collectively, our panelists have visited over 100 countries and have interviewed, been kidnapped or battled terrorists and freedom fighters on the front lines. Receive insights into the intelligence indicators within the Northern Alliance that served as precursors to the September 11 attacks, how terrorists are training and converging in the Tri-border region, and what the U.S. can expect in the continuing war on terrorism.

1:30PM–3:00PM

T2B: Innovations Track: Submit Your Ideas!

TRCcon is accepting proposals for two Innovations track slots. This is the perfect place to showcase your unique counterterrorism or homeland security concept or technology. Submissions should be sent to TRC@terrorism.com by August 15, 2003.

3:00PM BREAK

3:30PM–5:00PM

T1C: Primary Track: Terrorism Intelligence Analysis and Counterterrorism Operations

Sgt. John Sullivan, L.A. Country Terrorism Early Warning Group; Superintendent John Short, Detective Chief Head of Branch, Police Services of Northern Ireland; Superintendent Bill Lowry (retired), Former Chief of Special Branch–Belfast

Terrorism intelligence analysis is one of the greatest homeland security challenges we face. This session provides an overview of intelligence analysis and two case studies that serve as intelligence and counterterrorism operations models: the LA County Terrorism Early Warning Group and intelligence analysis techniques used against the IRA.

3:30PM–5:00PM

T2C: Innovations Track: Terrorism Indications and Warning: A Virtual Analysis System

Capt. Sundri Khasla, USAF

This session explores issues of intelligence analysis and the specific pitfalls associated with conducting Indications and Warnings (I&W) for terrorism. It proposes a methodology that uses proven analytical techniques and guards against nearly 80 percent of the 42 common warning pitfalls that experts have identified throughout history.

TRCcon DAY THREE—OCTOBER 3, 2003

8:00AM–8:30AM

KEYNOTE: HOMELAND SECURITY 2005

General Wayne Downing (retired)

The threat posed by terrorism is adaptive, which requires a dynamic response and homeland security posture. What will be the essential and publicly accepted elements of homeland security in future years and will it be enough to counter the anticipated threat?

8:30AM–9:30AM

TP2: PLENARY: Fourth Generation Warfare: Implications for Law Enforcement and Homeland Security

Dr. Robert Bunker

This session explains how understanding concepts of Fourth Generation Warfare are essential to homeland security and law enforcement. Modern terrorist adversaries have studied and applied elements of Fourth Generation Warfare that we must be prepared to address within our homeland security structure.

9:30AM–11:30AM

TP3: PLENARY: From Munich to Manhattan: Thirty Years of Counterterrorism Lessons Learned

Andrew Garfield, TRC and Kings College (London); Walter Purdy, Terrorism Research Center; Col. Sami Barak, Former Counterterrorism Advisor to Israeli Prime Minister; Special Guests

This session provides a historical overview of terrorism attacks over the past 30 years and how terrorists have adapted and innovated to present today's emerging threats. It also provides insight into how terrorists will adapt in the future and what lessons terrorists have learned in the post September 11th environment.

12:00PM–1:30PM LUNCH

1:30PM–3:00PM

T1D: Primary Track: Chem/Bio Threats and Response Panel

Dr. Don Ponikvar, Defense Group

Terrorist organizations have demonstrated an increasing interest in utilizing chemical/biological weapons for terrorist attacks. These experts discuss emerging trends, separating myth from reality and the implications on homeland security.

1:30PM–3:00PM

T2D: Innovations Track: Project Responder Knowledge Base

Don Hewitt, Project Responder Knowledge Base Program Manager

Where should First Responders go for information on counterterrorism and homeland security technologies, equipment standards, test and evaluation results, and equipment grants? Don Hewitt provides an overview of the Project Responder Knowledge Base, which provides a unified source of equipment information tied to National Terrorism Response Objectives and the Interagency Board's Standard Equipment List.

3:00PM BREAK

3:30PM–5:00PM

T1E: Primary Track: Homeland Security Risk Management: Insights from Industry

Steve Lucky, Director, Airline Pilots Association National Security Committee; Robert Sestrom, NYC Commercial Real Estate Owner; Other industry representatives to be determined

While the defense of the homeland falls within the domain of the federal government, the likely targets of attack, and operators of our critical infrastructure are private entities. Hear directly from industry regarding their security concerns and what programs they are putting in place to provide a balance between homeland security.

3:30PM–5:00PM

T2E: Innovations Track: Holistic Interoperability: An Integrated Response to Chemical/ Biological Attacks

This session provides an overview of the COBRA system for integrated response to chemical biological attacks, including analysis and lessons learned from recent terrorism response exercises.

Registration Form

September 30 – October 3, 2003
Renaissance Washington D.C. Hotel
Washington, D.C.

3 Ways to Register

1) Online at www.infowarcon.com or www.trccon.com
2) Fax: 203-840-9663
3) Mail: InfowarCon/TRCcon
c/o Reed Exhibitions
383 Main Avenue | Norwalk, CT 06851

☐ YES! Please sign me/us up! *(photocopy for additional registrations)*

1.
First Name _____ Last Name _____

Job Title _____

Affiliation _____

Address 1 _____

Address 2 _____

City _____

State _____ ZIP/Postal Code _____ Country _____

Phone (Do not include International dialing code) _____ Fax (Do not include International dialing code) _____

E-mail _____

We collect this data in order to provide you with information about InfowarCon and TRCcon and other organizations in your field. If you prefer not to receive further information, please see our privacy statement at www.infowarcon.com or www.trccon.com or call our privacy administrator at 1-888-306-2344 or outside the U.S. 1-203-840-5810.

2. Payment Information

Total Due $ _____

☐ Enclosed is check # _____

☐ Purchase order # _____

Charge to my:

☐ MasterCard ☐ VISA ☐ AmEx

Name (as it appears on card) _____

Card Number _____ Exp. Date _____

Signature _____ (I agree to pay the total amount according to my credit card issuer agreement.)

Registration cannot be processed unless accompanied by full payment. Cancellation policies apply.

CANCELLATION POLICY: Cancellations received prior to 08/25/03 are subject to a $100 service charge. Cancellations must be in writing before a refund can be processed. Cancellations after 08/25/03 and no-shows are subject to the full fee. Send cancellation requests to: c/o Reed Exhibitions; 383 Main Avenue, Norwalk, CT 06851.

3. To ensure enough seating, indicate which sessions you would like to attend.

InfowarCon — September 30 – October 3, 2003

September 30, 2003
☐ T1 ☐ T2 ☐ T3 ☐ T4 ☐ T5 ☐ T6

October 1, 2003
☐ P1 ☐ P2 ☐ P3 ☐ P4
☐ Session 1A ☐ Session 1B
☐ Session 2A ☐ Session 2B
☐ Session 3A ☐ Session 3B
☐ Session 4A ☐ Session 4B
☐ Session 5A ☐ Session 5B
☐ Session 6A ☐ Session 6B
☐ Session 7A ☐ Session 7B

October 2, 2003
☐ P5 ☐ P6 ☐ P7 ☐ P8
☐ Session 1D ☐ Session 1E
☐ Session 2D ☐ Session 2E
☐ Session 3D ☐ Session 3E
☐ Session 4D ☐ Session 4E
☐ Session 5D ☐ Session 5E
☐ Session 6D ☐ Session 6E
☐ Session 7D ☐ Session 7E
☐ Session 8A ☐ Session 8B

October 3, 2003
☐ T7 ☐ T8 ☐ T9 ☐ T10 ☐ T11

TRCcon — October 1–3, 2003

October 1, 2003
☐ P1 ☐ T1A

October 2, 2003
☐ TP1 ☐ T1B ☐ T2B ☐ T1C ☐ T2C

October 3, 2003
☐ TP2 ☐ TP3 ☐ T1D ☐ T2D ☐ T1E
☐ T2E

Event Registration Options

	Before 8/25/03	After 8/25/03 & Onsite
InfowarCon Conference *(Full InfowarCon conference on Wednesday and Thursday ONLY, does not include tutorials or TRCcon)*	$995	$1,195
TRCcon Conference *(Includes TRCcon conference and Wednesday morning plenary sessions ONLY, does not include InfowarCon conference or tutorials)*	$695	$795
InfowarCon & TRCcon Conference *(Full InfowarCon and TRCcon conference on Wednesday, Thursday and Friday)*	$1,495	$1,695
Two Tutorials *(Includes two tutorials on Tuesday and Friday ONLY, no InfowarCon or TRCcon Conference)*	$595	$695
One Tutorial *(Includes one tutorial on Tuesday or Friday ONLY, no InfowarCon or TRCcon Conference)*	$395	$495

For qualified Educational Groups, Military Educational Institutions, Group and InfraGard discounts, please call 727-360-4061.

Reed Exhibitions
383 Main Avenue
Norwalk, CT 06851

Priority Code: _____

PRSRT STD
U.S. POSTAGE
FPO
PAID
Reed Exhibition Companies

InfowarCon™

TRCcon 2003
Annual Counterterrorism & Homeland Security Conference & Expo