

# NDIA 15th Annual T&E Conference Draws Large, Diverse Crowd

## Translating Data into Information into Knowledge Into Understanding into Combat Decisions

COLLIE J. JOHNSON

**R**etired Air Force Gen. Larry D. Welch has a reputation for getting things done. In fact, the word around Washington is that if you don't want the study or program to succeed, don't ask Welch to lead it. His reputation preceding him, Welch, who is the current Director of the Institute for Defense Analyses and former Air Force Chief of Staff, set the tone as keynote speaker for the 15th Annual National Defense Industrial Association (NDIA) Test and Evaluation National Conference and Exhibition by giving the conferees a good dose of what he's known for: plain talk, common sense, and a keen grasp of what it takes to cut to the issues.

"Our hardest test and evaluation challenge," he told the conferees, "is not only how do we build systems/networks that we know where the information is flowing, but that we have assurance in the integrity of the information and we can control access to the information — that we can do all that without interfering with the timely availability of information to those people who need it."

On that note, hundreds of test and evaluation senior leaders and practitioners stayed to hear more at the four-day conference held in Las Vegas, Nev., March 8-11. And during that four days they not

only heard Welch speak on "Forging Information into Battlespace Decisions" and the importance of achieving Information Superiority, but also heard a large cross-spectrum of information and perspectives from DoD and industry leaders on three related topics: Test and Evaluation of Defense Information Systems, Information Warfare (IW), and Information Assurance (IA).

### Why NDIA's Emphasis on Information?

Recent headlines warned us of the destructive nature of the Melissa computer virus. Since August 1998, Y2K has earned a spot on the nightly news. Telephone outages recently rendered the Pentagon "speechless" for several hours.

The business of the 15th Annual NDIA Conference was to talk about information — a word that used to be fairly common, but in recent years has taken on a vocabulary of its own.

Is the United States under cyber attack? Are hackers a serious threat to our nation's defense and industrial information systems? Are our information systems being penetrated? Are these intrusions being detected? To what extent? Have there been serious attacks against the information systems that support our nation's critical infrastructures? What role does test and evaluation have in the IW/IA arena? And finally, if our nation is under cyber attack, what can we do about it?



FROM LEFT: PHILIP COYLE, DIRECTOR, OPERATIONAL TEST & EVALUATION (DOT&E), OSD, WELCOMES RETIRED AIR FORCE GEN. LARRY WELCH, PRESIDENT, INSTITUTE FOR DEFENSE ANALYSES, TO THE 15TH ANNUAL T&E NATIONAL CONFERENCE & EXHIBITION, LAS VEGAS, NEV., MARCH 8-11. COYLE WAS THE 1999 CONFERENCE CHAIRMAN. WELCH, A FORMER AIR FORCE CHIEF OF STAFF, SERVED AS KEYNOTE SPEAKER.



JAMES F. "JIM" O'BRYON, DEPUTY DIRECTOR, OPERATIONAL TEST & EVALUATION/LIVE FIRE TESTING, AND CHAIRMAN, NDIA TEST & EVALUATION DIVISION, SERVED AS CONFERENCE MODERATOR. "WE NEED TO CHANGE THE WAY WE'RE DOING BUSINESS IN IA AND IW," O'BRYON TOLD THE CONFEREES. "I DON'T WANT TO BE A VICTIM OF THE FUTURE — I WANT TO CHANGE IT ... AND IT'S GOING TO TAKE WORK."

*Johnson is managing editor, Program Manager magazine, Visual Arts and Press Department, Division of College Administration and Services, DSMC.*

These questions and issues were the backdrop of the 1999 conference. In addition to Welch as keynote speaker, this year's conference planners brought out the T&E community "movers and shakers" to grapple with the issues, starting with Philip E. Coyle III, the current Director of Operational Test and Evaluation (DOT&E), OSD, and Conference Chairman. Victor Sheymov, believed to be the highest ranking KGB officer ever to defect from the Soviet Union, grabbed everyone's attention as he related his experiences as the KGB's officer in charge of Soviet Cypher Communications abroad, and Jack Krings, a former Director of Operational Test and Evaluation, rounded out a rostrum of speakers that represented the best of the DoD-industry T&E community.

### Emphasis Changing

The Revolution in Military Affairs is changing the emphasis in military operations to interoperability, systems-of-systems, and information systems. Systems can no longer be tested only in a stand-alone configuration, but must be tested with multiple other systems, increasing the complexity of the tests and straining the capabilities of existing resources. Coyle acknowledges that the state of Test and Evaluation (T&E) capability in DoD has continued to decline.

Achieving DoD's Joint Vision 2010 goals, Coyle says, relies in part on the two unifying concepts of information superiority and full-spectrum dominance. In his 1998 Annual Report to the Congress, he unequivocally stated that "Information superiority and information assurance will become an important part of operational testing programs."

To do this, Coyle told the conferees that DoD and industry must join forces to ensure that all elements of the U.S. Joint Forces are able to: (1) work together smoothly; (2) work well as a system-of-systems; and (3) have confidence that the information base can be used with assurance.

### Keynote Speaker

What is Information Superiority? Welch started his presentation by telling the conferees what it is *not*: "We have become accustomed to referring to a thing we call information superiority, and counting on this thing we call information superiority to be a basic underpinning of a great many of the 21st century concepts that we all find exciting and effectively find vital and essential.

"I would suggest to you that if we define information superiority as knowing more, and having more information flowing into us, having better sensors,



“We are all ‘information junkies’ — our kids absorb and integrate more information every day than adults in almost any other culture. So it’s this business, it’s this ability to translate information into combat decisions that’s the real issue.”

—Retired Air Force Gen.  
Larry D. Welch



ROBERT C. KELLY, VICE PRESIDENT, APPLIED SYSTEMS DIVISION, BTG, GAVE A PRESENTATION ON "RED TEAMS AS A TOOL FOR INFORMATION ASSURANCE TESTING."



"JOHN E. 'JACK' KRINGS PRESIDENT, KRINGS CORPORATION AND FORMER DOT&E, OSD, PRESENTED AN INDUSTRY PERSPECTIVE ON INFORMATION ASSURANCE AND SERVED ON THE T&E FOCUS PANEL.

### **Former Soviet KGB Officer Tells NDIA, "I Think We're Wide Open"**

Victor Sheymov, former KGB officer responsible for security of the Soviet Union's KGB Cypher Communications abroad during the 1970s, defected to the United States in 1980 for ideological reasons. Since then, he has served as an NSA contractor, specializing in computer communications security. He is also author of the book, *Tower of Secrets*, published through the Naval Institute Press. Sheymov was the featured guest speaker at the NDIA 15th Annual T&E National Conference and Exhibition, March 8-11.

Victor Sheymov doesn't have a problem holding the attention of his audience. Conferees sat riveted as he related his background as a former KGB officer in the Soviet Union prior to the end of the Cold War. Defecting to the United States in 1980, he had a story to tell, and it is a fascinating one. As the KGB officer responsible for security of KGB Cypher Communications abroad during the 1970s, Sheymov's experiences and background were particularly related to the foremost topics of the NDIA 15th Annual Test and Evaluation Conference: *Information Warfare* and *Information Assurance*.

"What is happening is that with expanding technology, we simultaneously open up our vulnerabilities," Sheymov told the conferees. "Inadvertently, we give our opposition (whatever that is) a chance to attack us in a way which would have been unavailable if we didn't develop technology to that extent." He spoke of the four major areas of cyber security from his perspective:

#### **Defense Against Cyber Attacks**

Sheymov insisted that firewall technology just doesn't work. And our current strategy of putting patches on firewalls is becoming an exceedingly expensive proposition. "We have to start developing the new technology as soon as we can," he said, "because I don't know how long we can go down that spiral, spending huge amounts of money on patching firewalls, only to have hackers spend two days finding a way to penetrate them."

#### **Defense Against Electronic Attacks**

"I think we're wide open, and I think this is probably the most underestimated danger now ... we have to develop, again, something principally new [barriers], worthy of the new technology we are handling in terms of computers." Sheymov advised the conferees that it would be easier to put effort into future development of the protective technology, rather than trying to figure out exactly what is going to happen (and he warned them that it would be something bad – of that they could be pretty sure).

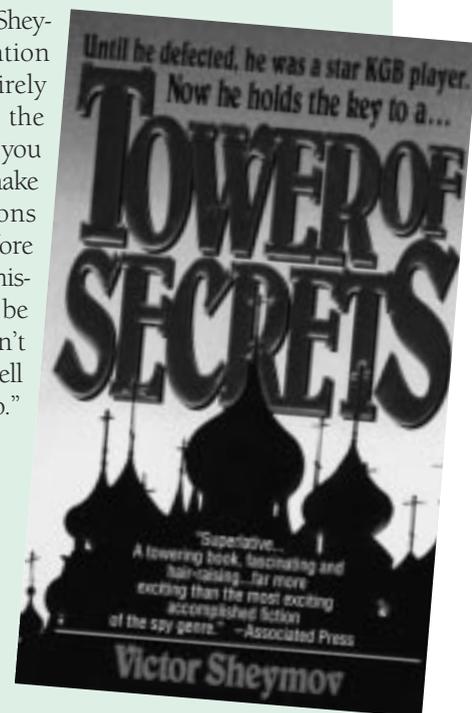
#### **Keyboard Access**

Keyboard access as it relates to computer security is actually in a little bit better state than the first two. However, he added one caveat to that assessment by saying, "I think it's in a pretty good state in the high-security environment. I don't think we have too many worries about that. However, if we look into a medium- or low-security environment, it is not in very good shape."

#### **Destruction of Information/Information Hardware Falling Into Enemy Hands**

This is an area Sheymov believes has not received nearly enough attention. What happens, he questioned, if our computer falls into the enemy's hands, suppose on the battlefield. That situation, he said, was a classic example of how our strengths can create vulnerabilities through development of technology. "I think (and I'm just shooting from the hip here), what I see as an opening in this particular area, is to take advantage of the near future technological developments, such as distribution of information. Instead of destroying the computer which falls into the enemy's hands, how about feeding false information to the enemy through the computer if we could develop an individualized capability of feeding information into computers."

Concluding his remarks, Sheymov said that his intention was not to paint an entirely grim picture. "We're at the plateau – the juncture if you will – where we have to make a few very hard decisions and think very hard before we make them, because mistakes at this stage could be extremely costly if we don't think hard enough and well enough about what to do."



having the ability to move more information to more places, then we will not be able to sustain information superiority.”

Information superiority, according to Welch, “is our nation’s ability to translate information into combat decisions,” a subject he acknowledges is enormously difficult to test and assess, but a subject that is vitally important.

Although Welch put before the conferees some hard truths, he also held out reason for optimism in the midst of the most critical T&E challenges this nation has ever faced.

### **Asymmetric Advantages**

Citing our “asymmetric advantages,” Welch said that this nation enjoys an enduring asymmetric advantage in terms of our ability to translate data into information into knowledge into understanding into combat decisions.

Calling it a cultural advantage, he says that “We are all ‘information junkies’ — our kids absorb and integrate more information every day than adults in almost any other culture. So it’s this business, it’s this ability to translate information into combat decisions that’s the real issue.”

Today’s defense environment, according to Welch, is characterized by absolutely relentless demand for a pace of transformation of the force in order to make this force capable of meeting the full panoply of 21st century needs for defense forces. Simultaneously, we [DoD] are facing an equally relentless demand for a perfect performance in the things we demand of the forces today, every day, all over the world.

In a nutshell, Welch contends that we are demanding that we transform our national military capabilities in totally new directions to meet a panoply of conditions that we have not experienced before, while maintaining near-perfect performance and currency. He characterizes that as “trying to change your shirt without taking off your jacket.” We have to do this transformation with “no breathing space,” he said, “and that’s what’s difficult. We’ve never been asked to do that before.”

### **Asymmetric Threats**

Welch spoke at length on asymmetric threats, which he defined as the impact from the velocity and scope of the availability of military capabilities and military information in the world’s arms bazaars, and “all these other things going on that make it possible for adversaries to buy for millions what required West-

ern investment of billions.” But here again, he delivered some good news along with the bad.

“Asymmetric threats are a fact of life and asymmetric threats are important, but I submit to you that there are also asymmetric advantages,” Welch told the conferees. He went on to say that the United States “enjoys asymmetric advantages, and it’s important as we [DoD] go through this period of transformation that we exploit these asymmetric advantages, that we protect these asymmetric advantages, and that we make these asymmetric advantages that which drives the outcome of the battlespace, whether that battlespace be an offshooting war, or whether it be peacekeeping, or whether it be humanitarian, or whether it be some other kind of operation.”

Drawing upon U.S. combat experiences during Vietnam and Desert Storm, Welch named five asymmetric advantages that he believed were particularly relevant to the subject of the conference:

### **PRECISION ATTACK**

During the air campaign in Vietnam, because of the very low lethality of the individual systems and the conditions under which U.S. troops operated, it was never possible to mass the lethality that would destroy the enemy’s infrastruc-



DR. MARVIN J. LANGSTON, DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR CIO POLICY AND IMPLEMENTATION, DEPUTY CHIEF INFORMATION OFFICER, OSD, PRESENTED A NATIONAL SECURITY PERSPECTIVE FOCUSED ON THE ONGOING, AND LARGELY UNRECOGNIZED CYBER WAR.



WALT HOLLIS, DEPUTY UNDER SECRETARY OF THE ARMY (OPERATIONS RESEARCH), SPOKE ON COMMON FLAWS IN INFORMATION SYSTEMS DISCOVERED IN OPERATIONAL TESTING.



WALT LABERGE, SENIOR RESEARCH SCIENTIST, UNIVERSITY OF TEXAS AT AUSTIN, PRESENTED A “NEW CONCEPT FOR HELPING INFORMATION-BASED PROGRAMS PASS OT&E.”

ture faster than they could repair it. Contrast that with Desert Storm. In Desert Storm a single fighter aircraft, or a single 120mm single round, or a single TOW missile from a Bradley could destroy, on a single mission, a militarily significant target.

#### AROUND-THE-CLOCK HIGH-INTENSITY OPERATIONS

Part of the reason why U.S. troops were unable to mass this kind of lethality for these low-lethality individual systems in Vietnam was because the enemy “owned the night.” U.S. troops could not operate effectively around-the-clock; consequently, night was the time for the adversary to regroup, reform, and then prepare for the next day’s combat. Contrast that with our fighter forces and our armored forces in Desert Storm – for those forces, night was the time of maximum advantage because of the ability to conduct precision attacks around-the-clock. Because of that ability, U.S. troops were able to maintain a pace of operations that simply overwhelmed what they thought was a fairly formidable enemy.

#### SUPERB COMBAT READINESS TRAINING

During Vietnam, Welch said that we sent soldiers, sailors, airmen, and Marines into combat in Vietnam that today would not be considered qualified to participate in a training exercise at the National Training Center. An example he gave contrasted the quality of training during Vietnam vs. the quality of training during Desert Storm.

During Vietnam, the conventional wisdom for a fighter or tactical aircrew in Vietnam was that if they survived the first 10 sorties, there was a good chance that they might become an effective combat air group. Contrast that with Desert Storm, where we expected Army, Air Force, Navy, and Marine aircrews to be totally effective on the first combat mission of their lives, at night, in the face of defenses of an order of magnitude more formidable than anything U.S. troops faced in Vietnam. “They met those expectations,” said Welch. “They met those expectations because of the quality of training and because of the quality of people.”

#### INFORMATION SUPERIORITY

The essence of command in the past has been, “How do you mass forces at the right place at the right time?” Welch maintained that most of us spend a significant part of our professional life learning how to do that and building the capabilities to do that, that is, to mass the right force at the right place at the right time. That takes good information, Welch said, and in many cases, the United States was totally unsuccessful in Vietnam. With Desert Storm came information superiority, and U.S. troops always knew more about what the opponent was doing than the opponent knew about what they were doing. In a very short time, the opponent was totally blind and had no way of stopping what U.S. troops were doing.

#### HIGH-QUALITY PEOPLE OF ALL RANKS

Commenting on the high quality of our people, Welch said it was best expressed by the Soviets. When a high ranking Soviet Marshall (who was the counterpart to our Chairman of the Joint Chiefs of Staff) came over here just before the Soviet Union landed on the dustbin of history, he spent 10 days being escorted around the United States by the Chairman of the Joint Chiefs and other members of the Joint Chiefs, meeting, talking to, observing U.S. soldiers, sailors, air-

men, and Marines working on a daily basis.

After he completed that experience he confided in his U.S. counterpart that he was not surprised by the quality of our equipment – he had understood that. He was not surprised by the quality of our officers – he had understood that. He was greatly surprised by the quality of our enlisted force, and more importantly, he was absolutely astounded by our confidence in, and our confidence from, our enlisted force; that is, in the relationship and the trust and confidence between all the ranks. On the way to New York City to catch his airplane back to Moscow, looking down he finally admitted, “I guess that probably comes from growing up in a democracy.”

#### Our Hardest Challenge

Naming our hardest test and evaluation challenge, Welch said that it is not only how do we build systems/networks that we know where the information is flowing, but that we have assurance in the integrity of the information, and we can control access to the information, and that we can do all that without interfering with the timely availability of information to those people who need it.

“This asymmetric advantage of quality and people that we can count on to lever-



HANK KLUPEFEL, SAIC, GAVE AN INDUSTRY PERSPECTIVE ON COUNTERING THE GROWING PROBLEM OF EXPLOITATION OF THE UNTRUSTWORTHINESS OF INFORMATION SYSTEMS.



PHILIP LACOMBE, VICE PRESIDENT, POLICY & COMMUNICATIONS, THE VERIDIAN CORPORATION, SPOKE ON THE RESULTS OF THE PRESIDENTIAL COMMISSION ON CRITICAL INFRASTRUCTURE PROTECTION (PCCIP).

age the capabilities we provide in that way," he told the conferees, "makes it in order of magnitude more important that we feed that system and exploit that system with the right kind of information that is readily translatable to knowledge and understanding and decisions."

### Warning — Information Overload

Information overload was another area that Welch said some people mistakenly equate with information superiority. "I have seen it reported that in the first 24 hours of Desert Storm, that Schwarzkopf's JTF [Joint Task Force] headquarters received and processed a million messages. And I suggest to you that while fusion and sorting is important to resolve conflicts between different sources of information, it is not the solution to information overload.

"The solution to information overload," Welch emphasized, "is simply don't do it. Minimize what we push at the commander and maximize their access to the information that they want, when they want it, at the pace they want it, in the quantity they want it, and in the form that they want it."

### Find Out What Works

Welch told the conferees that the central issue and challenge is how we first build the system, how we build the concepts,

and finally, how we can test and evaluate our ability to provide information and to use information in a way that translates into valid combat decisions. "How do we do that?" he asked the conferees.

There's an enormous amount that we must discover about what works, what doesn't work, and what it takes to make it work. According to Welch, every program is a challenge that requires experimentation. It requires figuring out what works. It's discovering the potential of using information in order to provide a pace of operations and overwhelming capability — precision operations. Inevitably, he believes, we will then structure the forces and the concepts and the organization to exploit that.

"We simply have to have trustworthy networks and trustworthy information," he emphasized, "because we will be betting the lives of soldiers, sailors, airmen, and Marines, and we will be betting the outcome of that particular liability."

Welch believes that maintaining the speed and pace of operations will ultimately enable U.S. forces "to provide the capabilities, because if we can do that — if we can sustain speed of operations, base of operations, precision operations, efficiency and effectiveness at the level that the potential suggests — then re-

gardless of how much information the adversary has, he simply will not be able to cope with that pace of operations."

### Conference Activities

As the week progressed, 58 speakers came from all walks of DoD and industry to share their unique perspectives and experiences on topics ranging from hacking techniques and countermeasures to vulnerability assessments; from a Presidential Commission report to a national security perspective; from common flaws in information systems to securing our nation's infrastructure; from Y2K to Red Teams.

In addition to a Town meeting and four focus panels, those attending the conference spent several hours each day discussing, disagreeing, building consensus, questioning, answering, and learning from the experts. DoD and industry exhibits also gave them a hands-on look at some of the latest information systems platforms and initiatives.

Tutorials were available on four topics: Information Warfare, Developing Information Assurance Requirements, Hacking Techniques and Countermeasures, and National Defense University (Industrial College of the Armed Forces) Information Warfare T&E Course. Those attending the tutorials were awarded certificates of course completion, which qualify toward the 80 hours of continuing acquisition education required for members of the Acquisition Corps every two years.

Also during the conference T&E Awards Luncheon, Coyle presented awards to the civilian, contractor, and military Testers of the Year, as selected by the Office of the Secretary of Defense, and Departments of the Army, Navy, and Air Force. The first award presented was a posthumous award to the **Army Government Civilian of the Year, Charles Cavana**. James Thornton, Cavana's son, accepted the award on his father's behalf. Other honorees included:

**ARMY MILITARY TESTER OF THE YEAR**  
Maj. Stephen M. Beatty, Advanced Concepts Test & Integration Directorate, U.S.



LOUIS J. "LOU" RODRIGUES, DIRECTOR, DEFENSE ACQUISITION ISSUES, NATIONAL SECURITY & INTERNATIONAL AFFAIRS DIVISION, U.S. GENERAL ACCOUNTING OFFICE (GAO), GAVE A PRESENTATION ON "RISK MANAGEMENT PRACTICES FOR SUCCESSFUL OUTCOMES."



DAVID S.C. CHU, VICE PRESIDENT, RAND CORPORATION, ARMY RESEARCH DIVISION, AND DIRECTOR ARROYO CENTER, SERVED ON THE TEST & EVALUATION FOCUS PANEL. CHU SPOKE ON HOW THE T&E COMMUNITY IS PERCEIVED BY THOSE IT IS INTENDED TO HELP.

Army Test & Experimentation Command

#### ARMY CONTRACTOR TESTER OF THE YEAR

Dr. David H. Brown, Battelle Corporation

#### NAVY MILITARY TESTER OF THE YEAR

Cmdr. David Alan Dunaway, Commander, Operational Test and Evaluation Forces (COMOPTEVFOR)

#### NAVY CONTRACTOR TESTER OF THE YEAR

Jerome C. Gehrig, PEO Cruise Missiles & Joint Unmanned Aerial Vehicles

#### NAVY CIVILIAN TESTER OF THE YEAR

Robert E. Dufresne, Naval Sea Systems Command (NAVSEA)

#### AIR FORCE MILITARY TESTER OF THE YEAR

Capt. Michael J. Geysler, 33rd Flight Test Squadron

#### AIR FORCE CONTRACTOR TESTER OF THE YEAR

David G. Bricker, 18th Flight Test Squadron

#### AIR FORCE CIVILIAN TESTER OF THE YEAR

Angelo Trunzo, 746 Flight Test Squadron

#### OFFICE OF THE SECRETARY OF DEFENSE CIVILIAN TESTER OF THE YEAR

Larry Miller (award accepted by Mario Lucchese on behalf of Miller, who was recovering from a serious illness).

The last day of the conference was a classified session at Nellis AFB devoted to threats and responses, and test and evaluation results for systems/systems of systems.

### Common Ground

Among the conferees, general consensus emerged on five key issues:

#### ISSUE 1

No system is safe, no firewall impervious, and no encrypted document exists for which the code can't be broken. All

“The solution to information overload is simply ‘Don’t do it.’ Minimize what we push at the commander and maximize their access to the information that they want, when they want it, at the pace they want it, in the quantity they want it ...”

—Retired Air Force Gen.  
Larry D. Welch

systems are subject to, will be, or are being penetrated. Deputy Secretary of Defense John Hamre has stated that we are “at war” in this area.

#### ISSUE 2

The problem with the cyber war is that DoD and the public at large don't generally accept the reality that this is a war and that it's ongoing. The country basically operates as if the reality is a minor inconvenience or doesn't exist. But as defense and the infrastructure start becoming almost one and the same (for example, 90 percent of defense communications are over commercial lines), the nation needs to start thinking about its defense as not one and the same, but at least dependent/interdependent with

the nation's infrastructure, whether it be the economic infrastructure, the financial infrastructure, or the industrial infrastructure.

#### ISSUE 3

Government and industry must work together to solve the Y2K problem; it must be “operationalized” and taken seriously at every level of command and throughout our nation's critical infrastructures.

#### ISSUE 4

The nation has become critically dependent on its information infrastructure. Even though the Deputy Secretary of Defense has stated the nation is “at war,” Congress and DoD have not yet committed the resources to fund IW/IA in proportion to the threat. Next year 25 people will have a budget of about \$20 million to address this problem — a problem that could bring this nation economically to its knees.

#### ISSUE 5

No one at OSD seems to be in charge of IW/IA. The apparent lack of a clear chain of command was mentioned consistently throughout the conference by individuals from the rank of lieutenant to major general and above. Clearly, the field does not understand who is in charge.

### This Is Real Work

General Larry Welch called IW/IA “a huge task in developing these capabilities and an even larger task in figuring out how to do that with test and evaluation.” He commended the IW/IA challenge to “NDIA and this room full of dedicated T&E practitioners,” stating that “This is a contest we can win if we focus on the right stuff, and we focus at the right intensity.”

At the close of the conference, James F. “Jim” O'Bryon, Deputy Director, Operational Test and Evaluation/Live Fire Testing, and Conference Moderator, best captured the mindset of NDIA and the conferees: “We need to change the way we're doing business in IW and IA,” O'Bryon told the conferees. “I don't want to be a victim of the future. I want to change it ... and it's going to take work.”