IDA Research Notes

IDA Studies and Analyses Center

Winter 2005

HOMELAND SECURITY

Issue Overview

Since well before the terrorist attacks of September 11, IDA has been in the forefront of producing studies and analyses supporting what has since come to be called homeland security and homeland defense. We have been an innovator in the fields of information- and cyber-security, U.S. critical information infrastructure protection, and U.S. counter-narcotics operations. Deterrence of trans-national actors and technical assessments of border security technologies have been transitioned to operational reality. These concepts have clear applicability to the evolving terrorist threat.

This issue of *IDA Research Notes* describes five of the more than 30 ongoing efforts at IDA that are directly related to homeland security. The Port Security study analyzes the classic terrorist strategy of leveraging our own infrastructure against us. The Electromagnetic Pulse paper describes a particular threat to civil infrastructure that is a metaphor for a larger class of threats; namely, disabling protective systems as a prelude to an otherwise manageable assault. Next, we discuss a number of Defense Planning Scenarios, which IDA helped DoD develop in order to assess gaps in DoD's capabilities to protect the United States from various terrorist threats. The fourth article on Dispersion Modeling describes IDA's role as an independent evaluator of the Hazardous Prediction and Assessment Capability (HPAC), which models the atmospheric transport of chemical, biological, or nuclear agents. Finally, the fifth article documents IDA's recent accomplishments regarding information sharing and information assurance for both DoD and the Department of Homeland Security.

In addition to these five studies, IDA is working on a wide variety of other efforts related to homeland security, including:

- Designing and managing an assessment infrastructure for the SAFETY Act.
- Providing analytic support for the DHS Office of National Capital Region Preparedness and Response Recovery.
- Analyzing options for point defense of critical infrastructure targets.
- Proposing methods for expediting first-responder technology transfer.
- Identifying remedies for infrastructure vulnerabilities in the financial sector.
- Identifying the requirements of a campaign-level response to campaign-style chemical/biological terrorism.
- Providing DHS with an implementation plan for the Federal Activities Inventory Reform (FAIR) Act.
- Helping to develop a homeland defense strategy and providing analyses to determine which capabilities that DoD currently provides to support civil authorities ought to be migrated to non-DoD agencies.

IDA has strong, diverse experience and expertise that is relevant to homeland security and defense, and we are helping sponsors deal with a wide variety of new and continuing challenges.

IDA
4850 MARK CENTER DRIVE
ALEXANDRIA, VA 22311-1882
TELEPHONE (703) 845-2000

INSTITUTE FOR DEFENSE ANALYSES

IDA's Studies and Analyses Center is a federally funded research and development center established to assist the Office of the Secretary of Defense, the Joint Staff, the Combatant Commands and Defense Agencies in addressing important national security issues, particularly those requiring scientific and technical expertise. IDA Studies and Analyses Center also conducts related research for other government agencies on national problems for which the Center's skills and expertise are especially suited.

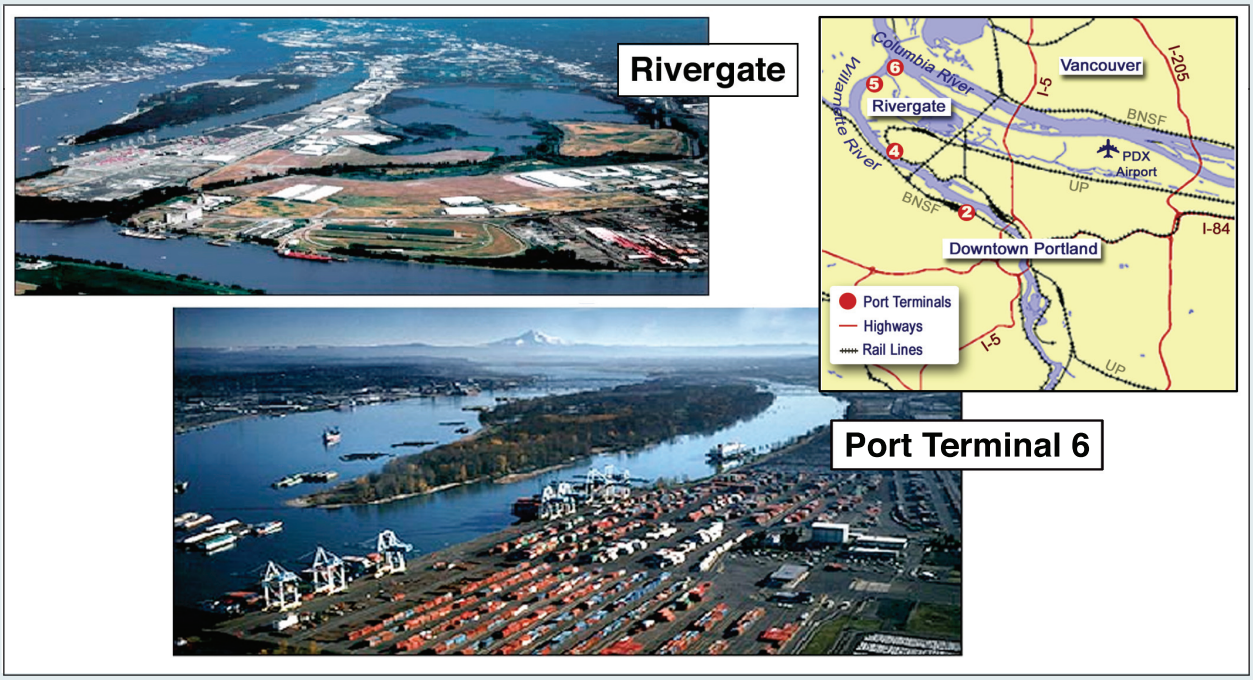
Port Vulnerability to Hazardous Chemical Incidents

by Gordon Boezer

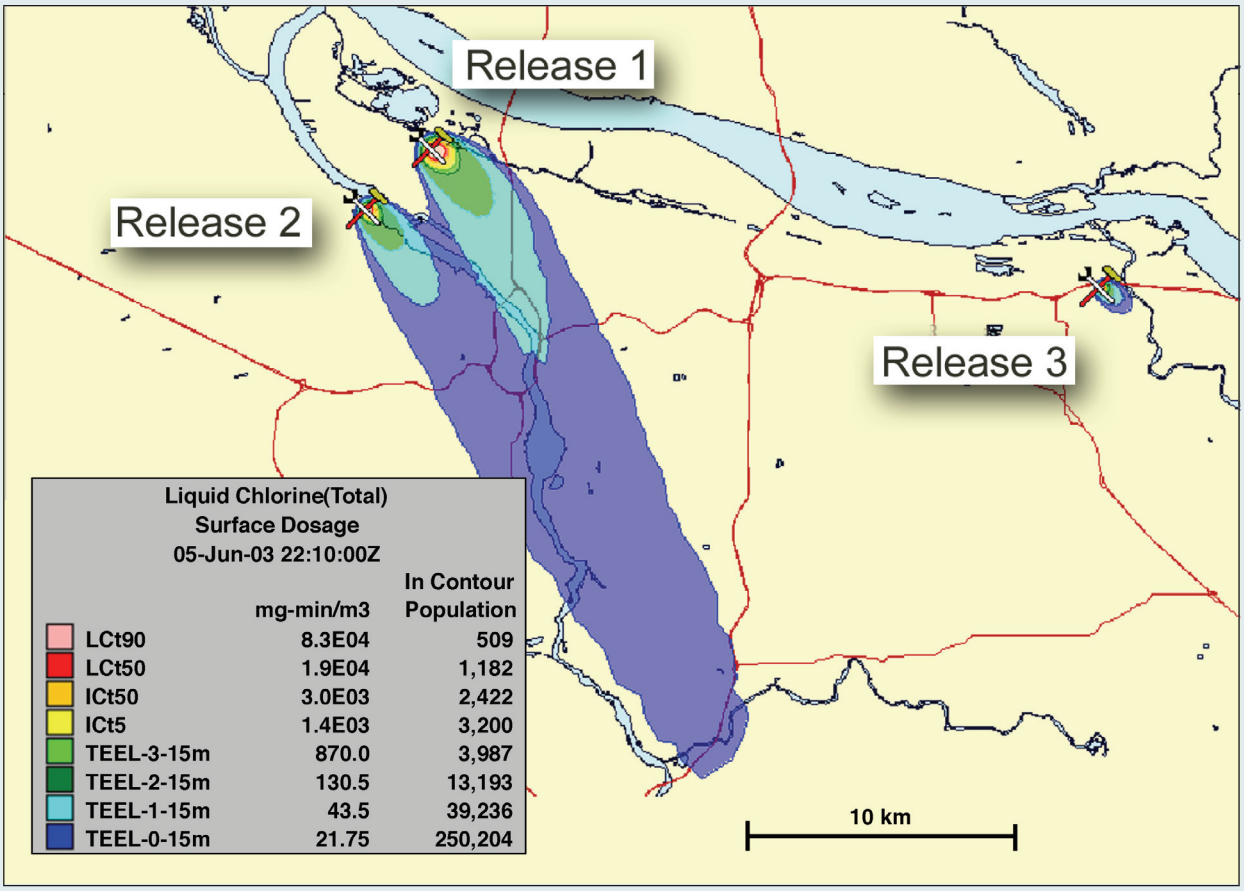
Publications by known terrorist organizations indicate that ports are potential terrorist targets. They speculate on the combined effects of a strike with explosives or other energetic material that release hazardous industrial chemicals into the port environment. The Department of Homeland Security's Advanced Research Projects Agency (HSARPA) engaged IDA to assist the Agency with thinking about investment in efforts to counter the effects of the release of hazardous chemicals should such an attack occur. HSARPA requested that the study be based on a port within the continental United States, preferably one hosting sea, air, and land transportation modes.

PORT OF PORTLAND

IDA selected Oregon's Port of Portland. This particular port covers a large geographical area as it extends from the mouth of the Columbia River at Astoria upriver approximately 100 miles to the end of the deepwater (40 feet) channel. Major wharfage and dock facilities are located within the city of Portland and at Astoria on the Oregon side and Longview, Kalama, and Vancouver on the Washington side. Portland is a major rail intersection for east-west and north-south rail traffic. In addition, interstate highways I-5 and I-84 intersect in Portland, and the Portland International Airport is near the Columbia River.



The Port of Portland covers a large geographical area, has major wharfage and dock facilities, and is located in a city intersected by major rail and interstate highway systems.



DTRA's HPAC model was used to analyze release plums of various toxic industrial chemicals. This figure shows the HPAC output for a compound chlorine scenario. The output shows the lethal concentrations (ICt), and temporary emergency exposure limits (TEEL). For example, the areas marked in yellow show the dosage of liquid chlorine that is lethal to 5% of exposed, unprotected personnel (LCt5). TEEL-1 predicts irritation and other minor effects, TEEL-2 predicts irritating but reversible effects, and TEEL-3 predicts serious impact and perhaps even death of compromised individuals.

The Columbia River itself is a major U.S. water transportation corridor, carrying more than 40% of U.S. wheat going to export markets. The river also conveys large volumes of newsprint, bulk ores, and processed minerals. Overall, Portland ranks 26th in total freight tonnage and 18th in container traffic. In 2002, 30 billion tons of international cargo moved through the port.

Of particular interest to this study are the port facilities that either handle or are in close proximity to large amounts of toxic industrial chemicals such as toluene, chlorine, anhydrous ammonia, caustic soda (sodium hydroxide), and sulfuric acid. In addition, north-south pipelines for petroleum products and natural gas service Portland from locations in the State of Washington and Canada.

The Port of Portland also provides a view of the economic consequences associated with closure. Over the years, the port has been closed by drought, flood, and the volcanic eruption of Mount St. Helens, which shut down the Columbia River system for two weeks. Members of the business community estimate that it has taken more than 20 years for

the port to recover the level of port business from shipping that was diverted to other facilities during that time. On the other hand, commercial operators are very supportive of emergency response activities that limit the impact of anything that could disrupt port operations.

EMERGENCY RESPONSE INFRASTRUCTURE

The U.S. Coast Guard Captain of the Columbia River ports is located in Portland proper. The FBI's regional center is in downtown Portland. The U.S. Army Corps of Engineers is responsible for waterway and dam maintenance. The nearest office of the Federal Emergency Management Agency is located 100 miles to the north in the State of Washington. Local officials indicated they are very much aware of both threats and hazards associated with toxic industrial chemicals. Table-top exercises, field activities, and training events have been held to respond to various types of incidents. IDA found, however, that improvements are needed in communications, equipment standards, and integrated training.

IDA worked with the Defense Threat Reduction Agency (DTRA) to assess the impact of a release of toxic industrial chemicals in storage or in transit through the port, using DTRA's Hazard Prediction Assessment Capability (HPAC) model to analyze release plumes for five scenarios. HPAC models the spread (or dispersion) of an outdoor plume of gaseous, aerosolized, or powdered material as a function of physical properties and atmospheric conditions.

Our analyses indicated that none of the five scenarios would totally close the port, though it did show cases in which the Portland metropolitan transportation system would become complicated by the closure of highway bridges and other transportation choke points. These disruptions would certainly hamper the movement of emergency responders and extend recovery time, but these effects were not specifically modeled. Informed speculation about the effects of releasing a chemical, such as VX nerve agent, in the port environment would cause one to expect a more serious disruption based on persistence and secondary spreading.

Regardless of whether the toxic material is a "routine" toxic industrial chemical or a chemical warfare agent that has been smuggled into the port, the port workers will be the first people to be affected by any incident. Their training and preparation can be key to providing deterrence and to limiting the effectiveness of any strike.

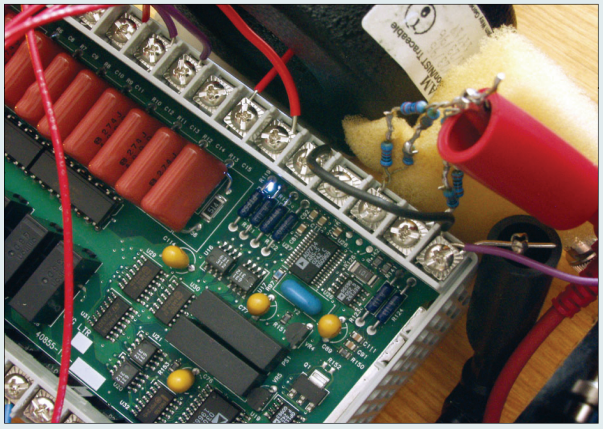
Our analysis also identified the limitations that must be overcome for the Department of Homeland Security to effectively communicate with locally based authorities. Bolstering communications–including addressing interoperability and security–among regional, state, and local authorities, first-responders, and federal officials would represent a major step forward in our ability to respond to the release of hazardous chemicals at a U.S. port.

Assessing the Threat to the United States from an Electromagnetic Pulse Attack

by James Silk

North America has by far the most reliable power in the world, yet we all have a passing familiarity with the consequences of short-term outages. In mid-August 2003, for example, one- to three-day electric power outages resulted from the Northeast Power Failure. Failures lasting as long as a week occurred due to severe thunderstorms in the Washington, DC area early that September, and Hurricane Isabel caused blackouts in the mid-Atlantic region, which in some limited areas lasted longer than a week.

All of these recent serious dislocations were the result of technical mishaps or natural phenomena. How much more debilitating consequences might result from an intentional attack? A coordinated physical attack on high-value assets such as generation plants and transmission substations could lead to widespread blackout in the short term, take years to repair, and create severe economic stress in the interim. Sporadic attacks on transmission line towers would incur huge financial burden. And the power system, like many infrastructures, is vulnerable to cyber-attack.



An electronic control unit undergoing HEMP vulnerability testing. The small electric arc near the center of the picture was enough to upset the operation of the unit.

As disturbing as these prospects may be, there is no scenario that is more threatening to the electric power infrastructure than a nuclear high-altitude electromagnetic pulse (HEMP) attack. Using known nuclear weapon technology, an adversary could generate a HEMP event that would directly disrupt an area several times larger than that affected by the 2003 Northeast Power Failure. This could be achieved using one or two weapons exploded in space, with no direct loss of life on the ground. The cascading effects from this disruption would almost certainly shut down the entire eastern or western interconnect.

The impact of such an outage would be severe, but not catastrophic, if the recovery were rapid. The recovery times from previous large-scale outages have been on the order of one to several days. This record of quick recovery is attributable to the remarkably effective operation of protective systems that are an essential part of the power infrastructure. In this context, the short blackout scenario would be painful, but not a threat to national survival.

INCREASED VULNERABILITY

The HEMP phenomenon has been understood for some time. Congress's recent interest in the subject can be attributed to two factors. First, in the context of peer bipolar superpowers, a HEMP attack was considered exclusively as a prelude to a nuclear exchange. Recovery from a standalone HEMP attack was not a compelling consideration. In a world of increasingly numerous non-peer proliferates, this calculus is no longer valid. Second, the United States' military and civil infrastructures are now much more reliant on digital electronic systems, which may place

the United States at an increased vulnerability to HEMP.

In light of this increased vulnerability, Congress created the Commission to Assess the Threat to the U.S. from Electromagnetic Pulse Attack, which was assembled and began work in 2002. IDA was asked to provide analytic support.

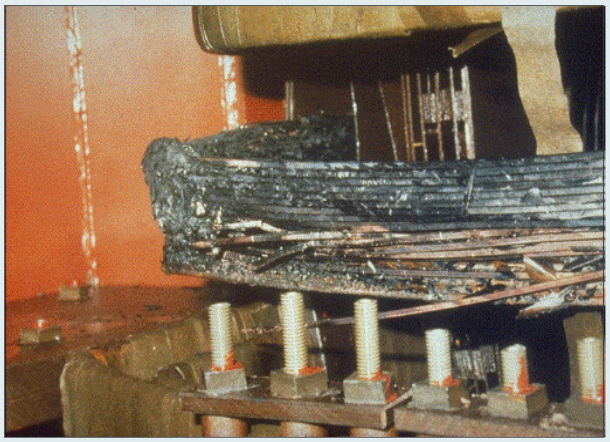
The Commission, established through Title XIV of Public Law 106-398, was to assess the following:

1. The nature and magnitude of potential high-altitude EMP threats to the United States from all potentially hostile states or non-state actors that have or could acquire nuclear weapons and ballistic missiles enabling them to perform a high-altitude EMP attack against the United States within the next 15 years.
2. The vulnerability of U.S. military and civilian systems to an EMP attack, giving special attention to vulnerability of the civilian infrastructure as a matter of emergency preparedness.
3. The capability of the United States to repair and recover from damage inflicted on U.S. military and civilian systems by an EMP attack.
4. The feasibility and cost of hardening select military and civilian systems against EMP attack.

While IDA played a key role in assessing all the civil and military infrastructures considered, this article focuses on the electric power infrastructure.

Early in its deliberations, the Commission began to compile infrastructure vulnerability to HEMP and assess prospects for recovery. It immediately became clear that the electric power sector is the lynchpin for recovery scenarios, due to the pervasive dependence of other infrastructures on electricity for normal operations and recovery.

The Commission then solicited technical assistance from the North American Electric Reliability Council (NERC), which was established in the aftermath of the 1965 Northeast Power Failure to assure the reliability of the grid. The NERC Board found that the Commission's concerns regarding the nature of the threat and the potential vulnerability were warranted, and it established a HEMP Task Force, under the aegis of its Critical Infrastructure Protection Advisory Group to provide technical advice to the Commission.



Protective systems usually can prevent damage to heavy equipment during power system upsets. However, this transformer suffered catastrophic failure during the solar storm that caused the HydroQuebec failure in 1989.

The Task Force, which was chaired by IDA on behalf of the Commission, included individuals with expertise on the three interconnects (Eastern, Western, and Southwest) and all three major grid components (generation, transmission, and distribution). Their guidance was essential for focusing the Commission and its staff on the importance of the early time HEMP pulse and its implications for grid recovery.

FINDINGS

The Commission, in collaboration with NERC, determined that in the early stages of the HEMP attack, before the grid collapse begins, the protective devices that have ensured past recovery could potentially be damaged. Over the last 20 years, the older electromechanical controllers and protective relays have largely been replaced by equipment containing electronic components. In the event of widespread electronic system failure, the grid would be unable to protect itself from the effects of cascading failure, leading to widespread damage to the generation, transmission, and distribution infrastructures. Rather than simply restoring power

to an intact infrastructure, the entire system would have to be repaired or replaced. It would take months or years to restore the system to a diminished but robust state, and decades to bring it up to current standards of electric power cost, access, and reliability.

As dire as these possibilities are, the Commission found early in its deliberations that the presumed susceptibility of modern electronic systems was based on little hard evidence. No comprehensive, independent testing of commercial electronics' hardness against HEMP had been done since the late 1980s. The Commission, therefore, sponsored new tests to assess the new generation of electronic control equipment that has since been put in use.

Although the assessment tested exemplars of most functional components, in most cases, due to expense and time constraints, typically only one vendor's equipment and only one or two samples of a type were tested. (Exceptions to this rule are noted below.) Three independent agencies conducted the tests, each using different approaches and protocols. When these agencies tested similar equipment, there was reasonable consistency in results, despite the differences in procedures.

The types of equipment tested and results in brief are as follows:

- **Electro-mechanical relays.** These are the "old fashioned" devices that contain no integrated circuits but function using high-power relays. They contain no digital electronics. They are still used in about 50% of applications, but that share is continuing to decline. As expected, these relays are immune to HEMP upset up to the highest levels tested.
- **Distribution line insulators.** Earlier studies had indicated high vulnerability for these simple devices. The 2003 tests indicate that there is indeed moderate vulnerability, but that it is not as severe as previously indicated.
- **Electronic protective relays and Supervisor Control and Data Acquisition (SCADA) remote terminal units.** These devices are essential for preserving high-value transmission equipment from damage during geomagnetic storms and other modes of grid collapse. Fortunately, these test items were the most robust of any of the electronic devices tested. However, both test agencies that assessed these devices reported that they are subject to upset at high levels of simulated HEMP assault. Altering the deployment configurations can further ameliorate the residual problems.
- **Programmable logic controllers and digital control systems.** These units are most commonly found in industrial settings and are extensively used in power plants. These are subject to upset and damage at moderate levels of HEMP assault.
- **General-purpose desktop computers and SCADA master terminal units.** These were the most susceptible to damage or upset of all the test articles. Unlike the other kinds of devices tested, several different models and vintages were examined by all three of the test agencies. The RS-232 ports are found to be particularly susceptible, even at very low levels of HEMP stress.

With the exception of the RS-232 connections, all of the electronic devices that were tested performed up to the manufacturers' claimed levels for electromagnetic compatibility. Thus, the international standards to which the manufacturers subscribe are being met, which indicates that these standards can be an extremely effective tool in a program to reduce vulnerability.

These results provide bad news and good news. The power grid is indeed vulnerable to collapse in a HEMP assault – primarily through the upset and damage that would be introduced through the soft computer systems that are in common use. For the particular protective relay and SCADA RTU that were tested, severe damage to high-value components would be limited by the hardness of the protective relay to the high end of the threat spectrum. However, the inherent hardness of these devices is known to be compromised when installation procedures do not take into account the possibility of HEMP assault. Such HEMP-inadequate installations are known to be commonplace. In these cases, robustness can be considerably enhanced at modest cost by attending to installation and configuration issues.

The Commission presented its report in testimony before the House Armed Services Committee on July 22, 2004. The report recommends a set of actions to limit the effects of a HEMP attack and, perhaps more important, to assure recovery in its event.

Planning for Homeland Defense Using Scenarios

by James Thomason

In September 2001, the Secretary of Defense announced a new force planning/sizing construct for the U.S. military, one going well beyond the two nearly-simultaneous major theater war force-sizing approach that prevailed through most of the 1990s. In his Quadrennial Defense Review (QDR) 2001 Report, delivered to Congress just days after the attacks of 9/11, Defense Secretary Donald Rumsfeld called for building U.S. forces and capabilities able to handle a sizable number of military missions concurrently. His overall approach has been branded the "1-4-2-1-1" concept of:

- Defending the U.S. against foreign attacks on the homeland ("1").
- Deterring aggression in four critical regions ("4").
- Swiftly defeating aggression in two major combat operations (MCOs) ("2").
- Being prepared to change the regime of one of those two MCO aggressors ("1").
- Conducting one (or more) smaller-scale contingencies ("1").

Protecting the homeland is the pinnacle of this defense preparedness agenda.

DEFENSE PLANNING SCENARIOS

IDA has recently assisted DoD in developing a number of Defense Planning Scenarios consistent with the 1-4-2-1-1 approach. One of these planning scenarios is focused entirely on defense of the U.S. homeland, circa 2012. This new Homeland Defense Scenario (HLDS) represents the first effort in many years to depict, in one place, a representative array of foreign challenges to the U.S. homeland against which DoD capability needs and programming priorities must be assessed.

While many specifics of this scenario are classified, representative threats range from foreign terrorists attacking with smuggled chemical, biological, and nuclear weapons to launches by states and, in some cases, by non-state actors, of several types of missiles against the U.S.

The organizing construct is that of a "layered defense." The principle is that DoD should aggressively develop and employ ways to prevent adversaries from:

1. Acquiring the dangerous weapons in the first place (for example, through U.S. counter-proliferation programs/initiatives).

2. Launching/using such weapons they do acquire (through U.S. pre-launch and launch-time disabling efforts).

3. Hitting U.S. targets with such weapons they are able to launch (through various U.S. post-launch destruction efforts).

4. Achieving as much damage as adversaries intend with any weapons that do hit U.S. targets (through point defense and other security measures, as well as robust consequence management approaches).

The HLDS articulates an integrated homeland defense concept; it forms the heart of a baseline strategy for addressing exceptionally serious potential external challenges to the United States in the years ahead.

The Defense Planning Scenario for homeland defense is already being used in several formal studies commissioned by DoD, providing explicit context for assessments of gaps in DoD's capabilities

and a formal test-bed for analyses of ways to close or minimize such gaps. IDA is conducting two of these studies.

ICCARM FRAMEWORK

In one study, the Integrated Cross-Capability Assessment and Risk Management (ICCARM) Framework, DoD asked IDA to develop an operational process by which the current force and the extant Future Years Defense Program force can be evaluated for how well they balance and mitigate strategic risk across major elements of the defense strategy and significant challenges that DoD must address. Threats posited in the HLDS comprise a key element of the overall "challenge space" in the ICCARM framework. Other prominent elements will include major combat operations, countering terrorism abroad, conducting stability operations, and handling several major types of "smaller-scale contingencies."

The ICCARM project also has constructed a range of increasingly transformational, equal-resource alternatives to the extant program force, options that show promise of better mitigating risks – including risks to the homeland— than the program force does. A pilot test of the ICCARM framework has now been completed.

NATIONAL DEFENSE STOCKPILE

In a second study, IDA is helping OSD assess the National Defense Stockpile (NDS) requirements for a wide range of non-fuel strategic and critical materials – from antimony through beryllium to germanium and zinc – using a scenario consistent with the U.S. defense strategy and with those DoD uses for regular planning and programming purposes. IDA is employing a three-step analytic architecture that we have developed for DoD over the last decade.

For this study, we crafted an overarching national security emergency planning scenario that is consistent with the 1-4-2-1-1 force-sizing construct.

This scenario uses the HLDS to guide development of a "representative nuclear attack" on a major U.S. city sometime in the next 5-10 years. Recovery from the damage sustained in such an attack is posited to include rebuilding critical infrastructure and property wherever feasible. These U.S. homeland recovery "demands" form an important part of the larger scenario being employed to determine whether the United States needs to maintain a multi-billion-dollar, national-level stockpile of strategic and critical non-fuel materials.

The Secretary of Defense will deliver his NDS Requirements Report to Congress in May 2005. The estimates in that report will be based in large part on demands derived from the HLDS, as well as from other Defense Planning Scenarios that IDA has crafted for DoD-wide use.

Beyond these two applications, the Secretary of Defense has tasked the Chairman of the Joint Chiefs of Staff to perform a major study of overall homeland defense requirements. This study, one of a number of analyses entitled Operational Availability 2005, is centered on the demands posed by the IDA-built HLDS; it will feature consideration of the layered-defense concept of U.S. operations articulated in that document.

Overall, the HLDS is being used intensively in at least three major studies this year, and our DoD sponsor expects that a version of this scenario will also be employed in DoD's wide-ranging Quadrennial Defense Review 2006, as well as in a broad set of studies by many DoD organizations in the years ahead.

Transport and Dispersion Models

by Steve Warner, Nathan Platt, and James F. Heagy

The Department of Defense must be able to estimate reliably how the release of chemical or biological agents would affect the population. Such estimates require knowledge of the concentrations of dispersed material as a function of time and location. The Defense Threat Reduction Agency (DTRA) has begun to augment its current Hazardous Prediction and Assessment Capability (HPAC) to include urban effects. To meet this challenge, DTRA has conducted field studies in which tracer gases were released within an urban environment to study flow and dispersion. DTRA asked IDA to analyze these tracer studies to compare the predictions of Urban HPAC to the observations of the Urban 2000 field trial.

The Urban 2000 field trials consisted of a series of sulfur hexafluoride (SF_6) releases that were carried out in the Salt Lake City area in October 2000. The data from these trials comprised meteorological and tracer measurements collected throughout the Salt Lake City urban region. For each of six intensive operating periods, three separate short-duration SF_6 releases were monitored for two hours. For each of these 18 separate two-hour monitoring periods, SF_6 samples were collected at 30-minute intervals at 66 ground locations.

HPAC PREDICTIONS

HPAC is a suite of software modules that simulate the release of hazardous agent, retrieve and prepare meteorological information prevailing at the time of the release, model the transport and dispersion of the hazardous agents over time, and plot and report the results of these calculations. Users can set HPAC surface type to "urban" to capture some of the effects of buildings on transport and dispersion. Urban HPAC also offers an urban dispersion model and an urban windfield module. Urban HPAC includes a building database that specifies the locations, planar geometries, and heights of buildings to support the calculation of flows in an urban environment. The windfield module predicts steady-state winds inside the urban region.

To evaluate the performance of the operational modules against the baseline configuration, we examined all four combinations of Urban HPAC switch settings:

- With an "urban" surface type (UC).
- With the urban dispersion model (DM).
- With the urban windfield module (WM).
- With both the dispersion model and windfield module (DW).

To test how dependent the HPAC predictions were on the fidelity of the input meteorological data, we examined the following five weather input options for each of the four switch settings (Figure 1):

- Surface measurements from the Salt Lake City airport, located about 10 km from the downtown area (SLC).
- Wind profile measurements from the Raging Waters site, located 5 km upwind of the release (RGW).
- Measurements from the top of the Latter Day Saints' administration building located within the urban area (LDS).
- All available meteorological measurements (ALL).
- An Operational Multiscale Environment Model with Grid Adaptivity forecast (OMG).

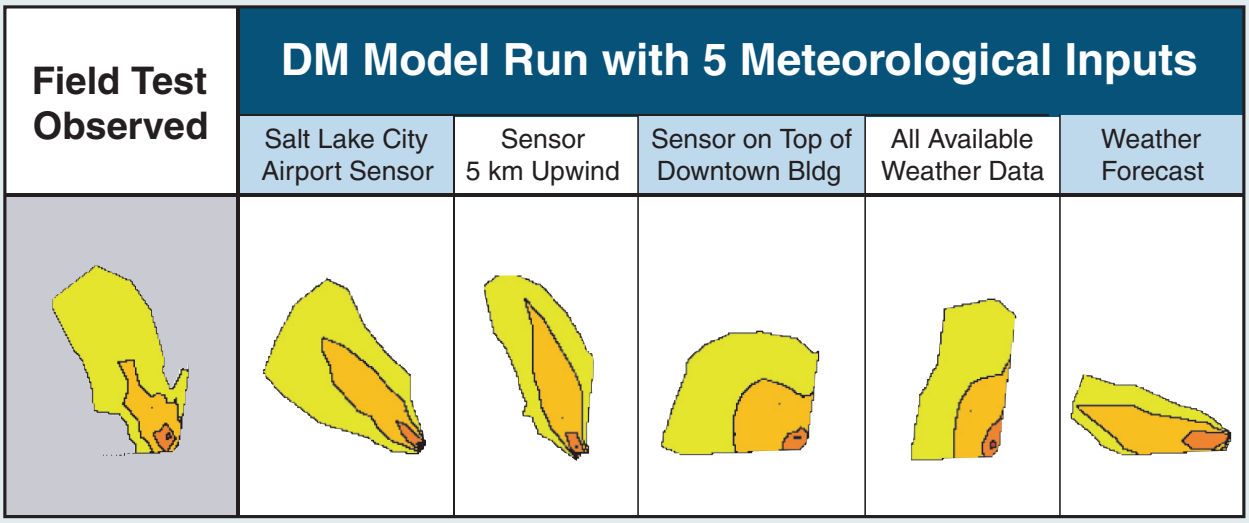


***Figure 1**. The figure shows a comparison of plumes (one observed and five predicted) for the release of a tracer gas in downtown Salt Lake City, Utah. In comparing different model configurations, it was important that a relative performance be assessed across a range of meterological input options.*

METHODOLOGY

IDA's analyses considered 4,752 (30-minute average) concentrations "paired in space and time" from the Urban 2000 field trials in making comparisons to the predictions of a given model. Unlike analyses based on derived, gross descriptors (e.g., "plume width" or "downwind distance"), this examination explicitly considers the size, shape, and specific location of the cloud. We expect these point-to-point comparisons to more accurately assess the ability of the models to represent realistic local effects.

We computed 13 statistical measures, along with their uncertainties, for each model configuration. Since we examined more than 25,000 comparisons, we needed to find an objective way to identify significant differences between model predictions. Using non-parametric hypothesis testing techniques, we looked for significant differences between models by making pair-wise comparisons (that is, two models at a time) of the statistic of interest for each of the 18 releases.

Figure 2 illustrates the value of this procedure for detecting significant differences. The point estimates and 95% approximate confidence intervals for the Fractional Bias are shown in Figure 2a for the four model configurations that used the "all available meteorological measurements" weather input option. The Fractional Bias statistic measure the average bias (over- or under-prediction) normalized by the observations and predictions. Figure 2a presents averages of the Fractional Bias for each model. Variations between model performances can be seen in this figure, but they are "within the error bars," so the statistical significance of these differences is not readily apparent.

Figure 2b shows the estimated mean Fractional Bias difference for the six comparisons that result from consideration of the four model configurations using all available weather measurements (ALL). Based on the averages in Figure 2a, one might expect all of these results to be consistent with zero. While the average behavior of the Fractional Bias statis-

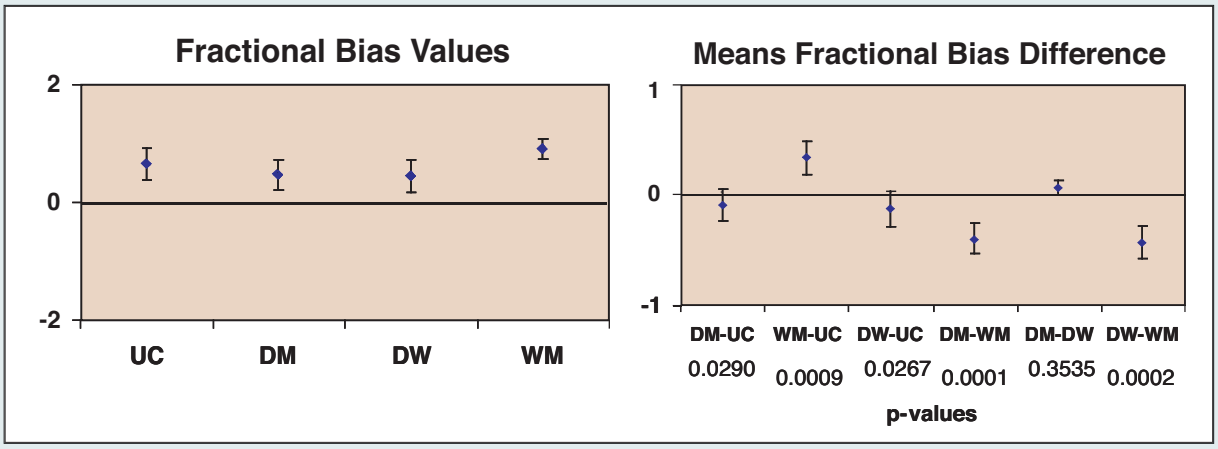


***Figure 2a**. Fractional Bias values for the four dispersion model configurations using the ALL weather input option. These values are based on model predictions of 30-minute average concentrations.*

***Figure 2b**. Mean Fractional Bias differences for the six model configuration comparisons. P-values result from non-parametric hypothesis tests.*

tics suggests that the models over-predict equally (within uncertainties), our pair-wise comparison on a test-by-test basis shows that the models are not equivalent. Thus, the pair-wise comparison allows us to refine our statistical significance. These results strongly suggest that the windfield module model configuration leads to significantly larger ("worse") Fractional Bias values relative to the other model configurations.

COMPARISONS OF MODEL CONFIGURATION

We found that the "best" predictions – those with less scatter – were, in general, associated with the Urban HPAC model that included the dispersion model (DM) switch toggled on. These findings relate only to these Urban HPAC predictions of Urban 2000. The predictions that included only changing the surface type to "urban" – "baseline" Urban HPAC – or included only the urban windfield module typically performed worst (with the exception of the urban surface type-OMG forecast configuration). In general, we found that including the windfield module with the dispersion model (DW) produced no significant improvements relative to using the dispersion model alone. When we used the OMG forecast weather input option, we found that the baseline Urban HPAC predictions that did not include the dispersion and windfield modules (UC) were best. An unusual finding was that the combination of the OMG weather input with the UC switch setting was consistent with zero Fractional Bias – it neither over-predicted nor under-predicted the measurements – even though (1) all 19 other combinations over-predicted the results, and (2) in all other weather input modules, UC performed worst (or tied for worst). Further investigation is required to determine whether this result is simply a matter of compensating errors.

CONCLUSIONS

Figure 3 provides a relative ranking of switch settings for each weather input. The ranking is based on model performance for all sampler locations. Best switch settings are on top, with statistical ties reflected as side-by-side positions. For four of the five weather input options, the DM predictions were ranked best or tied for best and the UC predictions were ranked worst or tied for worst. For the predictions run with the OMG weather input option, the exceptional result is that the UC_OMG

configuration is ranked as best. As discussed above, this combination outperformed all 19 others, but it is not yet understood whether this is fortuitous. Our study also examined model performance as a function of time resolution, model performance as a function of downwind distance, utility of the model to predict hazard locations, and the relative performance of the five weather input options. This independent validation study, along with ongoing IDA validation efforts, such as the Joint Urban 2003 Atmospheric Dispersion Study in Oklahoma City, will enable DTRA to make informed decisions within their urban transport and dispersion modeling program.

	Weather Input Options				
	Salt Lake City Airport Sensor (SLC)	Sensor 5 km Upwind (RGW)	Sensor on Top of Downtown Bldg (LDS)	All Available Weather Data (ALL)	Weather Forecast (OMG)
Model Configuration Ranking	DM , DW	DM	DM	DW, DM	UC
	WM,UC	DW	DW	WM	DM, DW
		WM,UC	WM	UC	WM
			UC		

UC – "urban" surface type
DM – urban dispersion model
WM – urban windfield module
DW – urban dispersion model and urban windfield module

Figure 3. *Rankings of Urban HPAC dispersion model configuration performance as measured by differences in scatter - Normalized Absolute Difference. Example: For the input option, the DM predictions ranked below UC, above WM, and not statistically different from DW. Also, note that for the ALL weather input option comparisons, the WM predictions could be ranked as below DM, above UC, and not statistically different from DW.*

Homeland Security and Information Technology

by L. Roger Mason

Information technology (IT) and the applied use of information underpin nearly every aspect of the homeland security mission, ranging from information sharing for combating terrorism to linking together 22 legacy agencies into a common information network. While IT has the potential to significantly advance U.S. capabilities in homeland security, it also represents some of the most difficult challenges.

IDA has been involved in the IT aspects of homeland security since the Department of Homeland Security's (DHS) beginnings as the Office of Homeland Security in the White House. Currently, we are working on both information sharing and information assurance issues as we help DHS deal with its overarching Homeland Security IT Strategy and the National Information Assurance Partnership.

INFORMATION SHARING

Information sharing takes many forms within the homeland security mission – from enterprise networking and services for DHS's 180,000 employees to the integration of highly sensitive terrorist information handled by the Terrorist Threat Integration Center. This requires experience in IT that spans technology, policy, and operational aspects. The DHS Information Analysis and Infrastructure Protection (IAIP) directorate asked IDA to assist DHS in a variety of information sharing and strategy activities.

In its National Strategy for Homeland Security (July 2002), DHS emphasized the importance of information sharing and systems and underscored the following priorities:

- Integrate information sharing across the federal government.
- Integrate information sharing across the state and local governments, private industry, and citizens.
- Adopt standards for electronic information relevant to homeland security.
- Improve public safety emergency communications.
- Ensure reliable public health information.

IDA's work for DHS initially is focusing on the first two priorities. One of our first activities was to assist DHS in establishing the concept, mission, and procedures for the Information Policy Board, which includes experts from government and industry. IDA has played a key role in identifying the issues that the board should tackle, including enterprise services (e.g., email, discovery, messaging), global network management, and information security. Recently, IDA helped DHS develop its "Terrorist Information Sharing Plan," which was drafted in response to President Bush's recent Executive Order (EO-13356) requiring agencies to complete their plans within 90 days.

While our work is ongoing, we have made significant early contributions to the DHS information sharing agenda, the impact of which has been felt across the department. The work will continue as IAIP addresses the complex multi-dimensional information integration challenges that will likely require new thinking as changes in the intelligence community emerge.

INFORMATION ASSURANCE

Federal government chief information officers (CIOs) point to information assurance as one of the most challenging problems in the IT environment. Because information assurance inherently relies on assets in the private sector, it is important for government and industry to work together to combat these threats. The known attacks to computer systems in the nation's critical infrastructure are increasing exponentially, with potentially far-reaching effects on homeland security.

Responding to security weaknesses in commercial software is a high priority of the National Information Assurance Partnership (NIAP). The NIAP is a joint effort between the National Institute of Standards and Technology and the National Security Agency to promote technically sound security practices, metrics, and evaluations of commercial IT products. The National Strategy to Secure Cyberspace (February 2003), which outlines a comprehensive approach for addressing information assurance challenges, directs that the NIAP be reviewed to determine its efficacy and to determine if its recommendations will help in the nation's information assurance efforts.

IDA was asked to lead the NIAP analyses in support of both DHS's Information Analysis and Infrastructure Protection office and DoD's Defense-wide Information Assurance Program (DIAP). We were asked to recommend future directions for the Partnership. IDA's long history of security evaluations for DIAP and others provided a solid foundation on which to base this effort. Our Team is taking the following approach:

- Forming independent fact-finding teams to investigate technology, policy, and processes.
- Interviewing individuals and groups from a sample population across the federal agencies and private industry.
- Conducting awareness workshops with a broad government and industry audience to ensure that all viewpoints are factored into the analyses.
- Synthesizing the collective key findings from each area to determine the multi dimensional dependencies and inter-relationships.
- Integrating the key findings with IDA security evaluation experience into a set of recommendations to improve the effectiveness of NIAP.

Having completed the major fact-finding phase, the team is currently analyzing the collected data. Many of the early findings exemplify the cross-dimensional aspects of the problems. For example, the pace of technological advances in software development methods (i.e., technology obsolescence) directly impacts the rigor and scope of the evaluation process, which is in-turn governed by the government policies on the use and application of the common criteria. The issue is further complicated due to the necessity of involving the international community.

As the analyses continue over the next several months, IDA will be working closely with DHS and DoD to recommend ways to improve the nation's ability to work with industry to produce more secure commercial IT products.

Other IDA Headlines

FUTURE COMBAT SYSTEM MANAGEMENT REVIEW

IDA reviewed the distinctive elements of the Army's Future Combat System (FCS) management approach and recommended ways to strengthen DoD's oversight of this complex program. Our study documents the major Army actions that have shaped the program, the selection of the industry participants, the terms and conditions of the agreement between the Army and Boeing Company to develop FCS "units of action," and the ethical environment established in both the government and industry. We found that the Army had adopted a conventional management approach for FCS that does not create unique risks for managing FCS development. At the same time, because FCS is a highly ambitious, risky program, we recommend additional management steps to address the program's many challenges.

IRAQI PERSPECTIVES PROJECT

IDA's Joint Advanced Warfighting Program provided valuable assistance in capturing lessons learned in Iraq in its Iraqi Perspectives Project. IDA collected and developed unique perspectives of major combat operations during Operation Iraqi Freedom from interviews with 15 of the top members of the former Iraqi regime and numerous senior military leaders, including corps and division commanders from the Iraqi Special Republican Guard, Republican Guard, and the Iraqi Regular Army. The program also draws on hundreds of captured Iraqi documents, including Iraqi assessments of most likely coalition courses of action, Iraqi lessons learned studies from the Operation Desert Storm, and Iraqi intelligence reports.

IMPROVISED EXPLOSIVE DEVICES

Several recent IDA projects have focused on developing and exploiting technologies for countering IEDs. We hosted a two-day workshop, which stressed the need for a "systems approach" aimed not only at finding and neutralizing emplaced IEDs, but also on attacking the full range of enemy activities that produces and deploys these devices. IDA also hosted two technology workshops that focused on methods of detecting IEDs before they can be detonated. The first of these workshops concentrated on determining how well IEDs can be detected using the systems and sensors that have been developed by the Army for countering landmines. The second discussed detecting IEDs by directly sensing their explosive content. IDA scientists also have studied other defeat mechanisms that could apply to many IEDs, including detection of radio-controlled fusing devices as well as detection of other signatures that may be unique to IED threats.

JOINT STRIKE FIGHTER REVIEW PANEL

An IDA assessment of the Joint Strike Fighter (JSF) noted that the JSF will provide a significant step forward in survivability, reliability, and maintainability, while providing a common platform for a new generation of mission systems. However, higher-than-estimated system weight, particularly for the short take-off and vertical landing variant, is a major issue that must be resolved before the aircraft enters production. For this project, IDA calculated an independent weight estimate for each JSF variant, noted how the weight would impact performance, evaluated several options for addressing the problem, and then recommended actions for improvement.

URBAN RESOLVE: A HUMAN-IN-THE-LOOP EXPERIMENT

IDA designed and conducted Phase I, a human-in-the-loop (HITL) experiment to explore future joint urban operations in 2015 – 2020. Urban Resolve, a three-phased HITL experiment, examined (1) how to gain situational understanding in the urban

battlespace; (2) how to isolate, control, and shape that battlespace; and (3) how to maneuver and support joint forces to engage and defeat enemies in urban areas. Phase I of Urban Resolve explored a combination of future high-, medium-, and low-altitude sensors on unmanned air and ground vehicles, coupled with unattended ground sensors and a covert human intelligence network, against an adaptive Red force attempting to hide, deceive Blue forces, and prepare defenses against an impending Blue attack. Preliminary analysis indicates that sensors deployed on low-altitude unmanned air vehicles and the ability to "tag" Red personnel and vehicles were critical to the success of the concept.

COMBATANT COMMANDER SUPPORT PROGRAM

IDA launched a pilot program in support of Combatant Commanders consisting of two IDA research staff members stationed at U.S. Pacific Command (PACOM) headquarters in Hawaii. The IDA team is assisting with communications among PACOM and OSD, Joint Staff, JFCOM, and Defense Agencies; facilitating collaboration among the various Combatant Commands on similar issues and processes; improving IDA research staff's awareness of current operational issues; and leveraging IDA's ongoing efforts to assist PACOM. The overall goal is to help speed the introduction of new capabilities into operational units.

NATIONAL PERSONNEL RECOVERY ARCHITECTURE

DoD is developing a National Personnel Recovery Architecture that considers the recovery of U.S. government civilians and contractors, in addition to U.S. military personnel, if they are isolated behind enemy lines or captured. IDA was asked to assess existing capabilities, develop a vision for personnel recovery, identify current shortfalls, and propose corrective steps to achieve a national architecture, including the required funding. We recommended the following: 1) promulgate a National Security Presidential Directive on personnel recovery to establish a coherent and cohesive architecture that includes all U.S. government departments and agencies; 2) initiate a program within the Department of State to enhance U.S. embassies' readiness for personnel recovery incidents; 3) standardize the government contracting process for personnel recovery coverage for contractors; and 4) improve personnel recovery training of DoD and non-DoD individuals.

CONTINGENCY OPERATIONS SUPPORT TOOL

IDA's Contingency Operations Support Tool (COST) provides an automated, common basis for DoD's financial and resource management community to estimate the costs of contingency operations worldwide. Using the COST model, DoD analysts can create a rough initial cost estimate in the early stages of planning when relatively little is known about an operation, followed later by more detailed estimates as additional information becomes available. In FY 2004, IDA's COST development team refined the model to enable better estimates of the costs of ongoing operations in Iraq, Afghanistan, and elsewhere. More than $115 billion of supplemental funding requests through the summer of 2004 were derived using COST. DoD has mandated that COST be used as a common estimating platform for reimbursing all Service and agency war-related costs.

LESSONS LEARNED: MAZAR-E SHARIF

In October 2001, Special Operations Forces in Afghanistan linked with the Northern Alliance and directed precision weapons from the air to defeat the Taliban in the area around Mazar-e sharif. The battle was key to the coalition force victory in the north and ultimately its success in Afghanistan. At the request of the Combatant Commander, U.S. Central Command, an IDA/DARPA team collected data from the battlefields and, using state-of-the art simulation tools, reconstructed selected events from the Campaign for Mazar-e Sharif as an "instructional tool for future leader development" and to support historical analysis as well as facilitate further research and development of irregular warfare.

Selected Articles from Past Issues

Systems Evaluations

- AIM-9X: A Modeling and Simulation Success Story *(2001)*
- Assessment of Airlift Requirements *(2000)*
- Assessment of Lethality Enhancement Alternatives for the AC-130 *(1999)*
- COATS: A New Approach to Submarine Testing *(2003)*
- Evaluation of Long Range Fire Support Systems *(1998)*
- Evaluation Plan for the Navy's Area Theater Ballistic Missile Defense System *(1997)*
- Integrated C4ISR Analytical Tool Set *(2001)*
- Naval Expeditionary Warfare Maneuver, Planning, and Execution *(2003)*
- New Initiatives for Operational Test and Evaluation *(1999)*
- Realistic Testing: Key to F-22 Mission Effectiveness *(2002)*
- Simulation in Support of Live Fire Test & Evaluation *(1999)*
- Small Combatants: Implications for Effectiveness and Cost of Navy Surface Forces *(2003)*
- Strategic Airlift: IDA's C-5 Modernization Study *(1998)*
- Surface Ship Radars *(2003)*
- Testing the Navy-Marine Corps Intranet *(2003)*

Technology Assessments

- Advanced Distributed Learning (ADL) *(2000)*
- Assessing the Future of the Global Positioning System *(2000)*
- Defense Electronics: Keeping the Edge *(2000)*
- Digital Representations of the Environment: Requirements, Representations, and Constructions *(2000)*
- IDA Support for the Global Combat Support System *(2000)*
- IDA Hosts Workshop on Advanced Technologies and Future Joint Warfighting *(1999)*
- MicroElectroMechanical Systems – Prime Enablers of Future Weapons Systems *(1998)*
- Militarily Critical Technologies Program *(2004)*
- Quantifying Military Information *(2001)*
- Smart Materials and Structures… or "It's a bird! No, it's a plane…" *(1999)*
- Technology and the Challenges of Defense Training *(1999)*
- The MOUT ACTD Analysis and Technology Assessment *(2000)*
- Warfighters' Edge: Using Intelligent Agents to Solve Warfighter Problems *(2002)*

Resource and Support Analyses

- Cost Analysis for the Airborne Electronic Attack Analysis of Alternatives *(2003)*
- Cost Estimating for Next Generation Aircraft *(2000)*
- IDA Builds Capability to Evaluate Industrial Base *(1998)*
- IDA Course Strengthens Acquisition Workforce's Understanding of Operating and Support Cost Analysis *(2002)*
- IDA's Role in the President's Commission on Critical Infrastructure Protection *(1997)*
- Idle Capacity in Aircraft Plants: How Much Is DoD Paying? *(2002)*
- Reducing Defense Infrastructure Costs *(2000)*
- Strengthening Defense Resource Management in Emerging Democracies *(2004)*
- Synthetic Environments for National Security Estimates (SENSE) *(1998)*
- The Contingency Operations Support Tool (COST) *(1999)*

Force and Strategy Assessments

- Attack Operations against Critical Mobile Targets *(2000)*
- Confronting the Threat of Chemical and Biological Weapons: IDA's Chem/Bio Program *(1998)*
- Counterdrug Research *(1998)*
- Crisis Management Engagement Activities in Southeastern Europe *(2004)*
- Enlarging NATO: Opening Options for Aspiring Members *(2004)*
- IDA Studies of National Security Organizations and Management *(2000)*
- Quadrennial Defense Review Analysis *(2001)*
- Regional Implications of U.S. Policy Options for North Korea *(2004)*
- Taking the "Revolution in Military Affairs" Downtown: A DoD Roadmap for Improving Capabilities for Urban Operations *(2002)*
- The Psychology of Deterrence – A Quantitative Model *(2000)*

4850 MARK CENTER DRIVE
ALEXANDRIA, VA 22311-1882
TELEPHONE (703) 845-2000

INSTITUTE FOR DEFENSE ANALYSES