

SPECIAL EDITION

CENTER FOR DEFENSE TECHNOLOGY AND EDUCATION FOR THE MILITARY SERVICES (CDTEMS)

The United States military is faced with a difficult environment; maintaining current military strengths while transforming the military services to meet the required capabilities-based emphasis for future funding, and while significantly improving homeland defense. The long term impact of emerging technologies on successful joint warfighting, the effects of homeland defense requirements on the required technologies and on national defense strategy, and the education requirements of the military forces to effectively utilize these emerging technologies and strategies are not currently being addressed to the level required for rapid transformation.

To address the above issues CDTEMS was formed in FY00 with Congressional support. This funding was continued in FY01. However, most of that funding was subject to approval by USJFCOM J9 and therefore had to be directed at programs that supported the J9 mission. In FY02 the funding came directly to NPS, permitting us to initiate innovative new programs in support of CDTEMS objectives. The above stated focus of CDTEMS is especially important after the events of 11 September. Since the private sector has surpassed DoD in their ability to rapidly develop and apply technology and since the DoD is no longer the primary developer of new technology, DoD must effectively leverage their S&T investments in critical areas to insure our continued superiority in military capabilities. It must also use new and innovative incentives and educational methods to encourage more young warfighters to focus their education on science and engineering so that they can more effectively utilize these new technologies. Many of the new technologies are multi-disciplinary and require systems analyses.

In FY01 CDTEMS funding for the NPS Program was utilized to support the formation of three new Institutes; the Cebrowski Institute for Information Innovation and Superiority (CI), the Modeling, Virtual Environments, and Simulation Institute (MOVES), and the Wayne E. Meyer Institute of Systems Engineering (MI). These education and research Institutes are highly interdisciplinary in approach and address many of the stated objectives of CDTEMS. The CI is the center of innovative research and education in enabling information technologies, operations, and strategies, with focus on their development and application for national security. Using

--continued on page 2

IN THIS ISSUE

Center for Defense Technology and Education for the Military Services

The Nemesis Project: Concept of Operations3

Network Management for Ubiquitous Surveillance Environment6

Integrated Asymmetric Goal Organization (IAGO): A Multi-Agent Model of Conceptual Blending.....8

Integrated Project in Expeditionary Warfare Complete Major Milestone12

Information Operations Summer Study15

Monterey Summer Study: U.S. Defense Policy Options for South Asia.....16

Design, Performance and Analysis of Unmanned Aerial Vehicle Systems Short-Course16

Strategic Insights17

Demonstration of Linked Unmanned Aerial Vehicle (UAV) Observations and Atmospheric Model Prediction in Chem/Bio Attack Response.....19

Fleet Transit Program22

Laser Beacon Prototype22

Integrated Theater Assessment Profiling System ..24

Shipboard Integrated Tactical Team.....26

Experimental Analysis of the Integration of Unmanned Aerial Vehicles and Naval Special Warfare Operations27

Homeland Defense and Security: The Naval Postgraduate School's Initiative

Homeland Security Digital Library Project.....33

Attacking and Defending Communications Networks.....34

Face Recognition System Using Uncooled Infrared Imaging.....36

Analyzing Electric Power Grids Under Terrorist Threat38

Vulnerability of Wireless Local Area Networks to Interception40

Concealed Weapons Detection.....41

Intelligent Software Decoys42

NPS RESEARCH is published by the Office of the Dean of Research in accordance with NAVSO P-35. Views and opinions expressed are not necessarily those of the Department of the Navy. Comments/inquiries can be addressed via email to research@nps.navy.mil.

NAVAL POSTGRADUATE SCHOOL
RADM David R. Ellison, USN, Superintendent
Dr. Richard Elster, Provost
Dr. David W. Netzer, Associate Provost and Dean of Research
Danielle Kuska, Editor, NPS Research

CDTEMS, *continued from page 1*

partnerships with industry and academe as appropriate, it also provides Information Professional education and innovative technologies for the warfighter by conducting research in the areas of network infrastructure, fixed and mobile technologies, computer and network security, software systems and interfaces, strategic operations and applications, educational technologies, and policies and management. The MOVES

Institute is focused on research, application and education in modeling, virtual environments, and simulation. Its research focuses on 3D visual simulation, networked virtual environments, computer-generated autonomy, human performance engineering, immersive technologies, defense/entertainment collaboration, and operational modeling.

The MI provides unique graduate education and research

to increase the knowledge and skills of military officers and the supporting civilian force in systems engineering, systems analysis, and large-scale experimentation. In addition to applied research in these areas, this Institute sponsors a campus-wide interdisciplinary systems engineering project that addresses force-level issues. In the past these studies have included the value of UAV aircraft carriers and small inshore combatants. Funding in FY01 was also utilized to form a new Research Center, the Center for Contemporary Conflict (CCC), whose initial effort was an innovative new program to bring focused regional security education to deploying forces.

In FY02 CDTEMS continued to support innovative programs within the three Institutes. The CI initiated a new project/capability called NEMESIS which will be a fully reconfigurable mobile computer network attack/defense and exploitation and research platform. As a part of this effort the Global Information Grid Applications (GIGA) Lab was enhanced to provide a network operating center and modeling and simulation support for the mobile van. In MOVES a new center was formed; the Center for the Study of Potential Outcomes. Its initial project focused on a multiagent model of conceptual blending in which agent technology can create new knowledge based on its experience and processing. The

goal is to provide a computational model which can contribute to better anticipation of asymmetric threats such as terrorist behavior. The MI year-long student project was a systems study of Expeditionary Warfare. CDTEMS also embarked on several additional new programs; a summer study to review all Information Operations (IO) education that is currently

available and to provide a proposed education program for Information Operations (IO) in accordance with Defense Planning Guidance (DPG), another summer study which examined U.S. defense policy options for South Asia, development of a comprehensive short course which addressed a critical emerging area for the warfighter—Unmanned Aerial Vehicles, augmentation of the CCC program to develop Strategic Insights which provide web-based, concise monthly analyses of regions and issues

critical to U.S. national security, an interdisciplinary program to demonstrate the utility of combining meteorological and oceanographic (METOC) prediction capabilities with UAV sensor measurements and flight control for rapid decision making required when Chem/Bio agents are released, an innovative Fleet-Transit program in which faculty and students are able to evaluate some of their latest science and technology and demonstrate its value to the Fleet as it transits off the Monterey coastline, a student fellowship program which permits our students to utilize knowledge and experience with current operational shortfalls and work on solutions using their thesis research effort, and a limited objective field experiment to demonstrate the utility for utilizing multiple, expendable, small UAVs with Navy Special Forces (SEALs) for enhancement of the downed-pilot-rescue mission. Each of these efforts is discussed in this issue of the Research Newsletter.

CDTEMS has provided a valuable new capability to NPS. We now have the funding which gives us the flexibility to utilize the knowledge and skills of our unique joint and international students and of our faculty to investigate innovative new approaches for applying emerging technologies and educational methods to enhance warfighter effectiveness.

Since the private sector has surpassed DoD in their ability to rapidly develop and apply technology and since the DoD is no longer the primary developer of new technology, DoD must effectively leverage their S&T investments in critical areas to insure our continued superiority in military capabilities. It must also use new and innovative incentives and educational methods to encourage more young warfighters to focus their education on science and engineering so that they can more effectively utilize these new technologies. Many of the new technologies are multi-disciplinary and require systems analyses.

THE NEMESIS PROJECT: CONCEPT OF OPERATIONS

Introduction

The Cebrowski Institute for Information Innovation and Superiority (CI) Network Warfare Van (NetWarVan) program is called the "Nemesis Project." The purpose of the Nemesis project is to create a fully re-configurable mobile computer network attack/defense and exploitation lab and research platform to ensure NPS's role as a dominant resource for years to come in the wireless Information Assurance space. Nemesis's initial configuration will be as a mobile 802.11 wireless computer network vulnerability lab and research facility. The Nemesis deployment platform will be re-configurable to allow for research and development of solutions for vulnerability assessment for several other emerging wireless communication mediums such as cellular phone communication vulnerability research, fixed broadband wireless data vulnerability research, and other radio frequency (RF) vulnerabilities. A byproduct of this initiative will be to create and implement a Computer Network Vulnerability Assessment Training portal via a secure website on the SIPRNET for USPACOM and other major DoD organizations.

Background

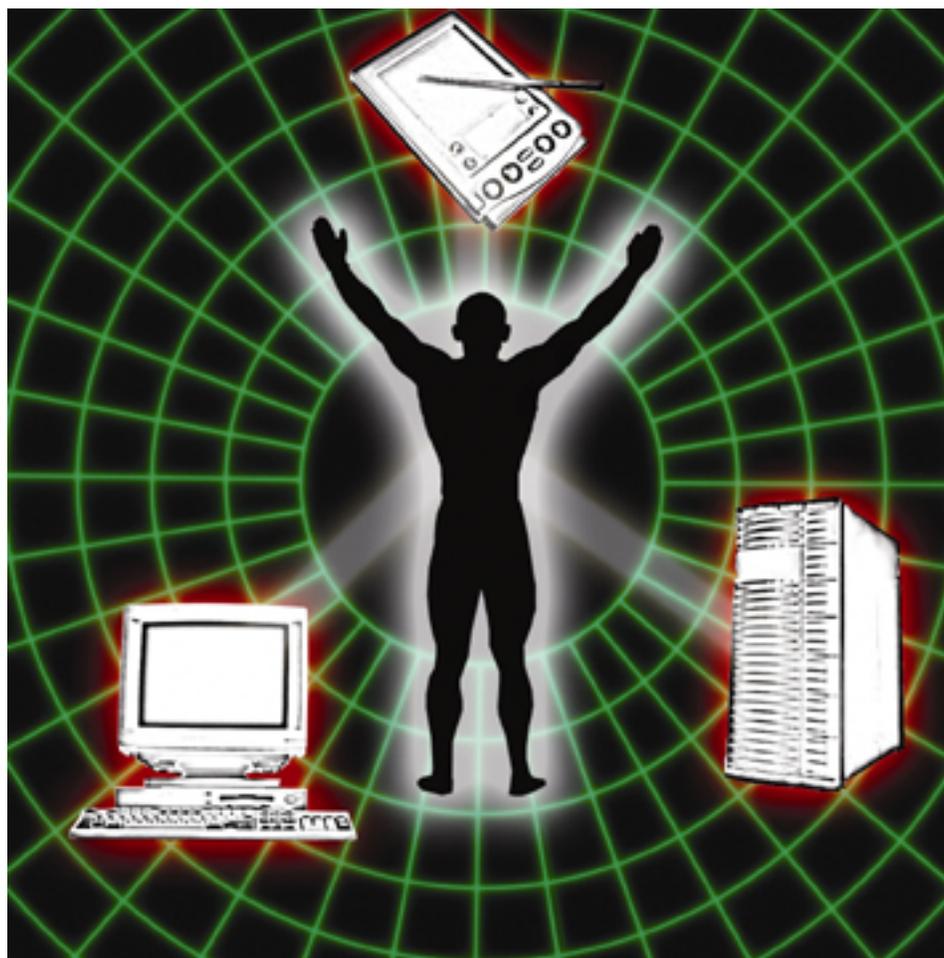
With the recent proliferation of wireless (802.11) networks in DoD and in the Federal Government, many of which are ad hoc wireless networks with little or no command coordination/knowledge and consideration for security, comes a dramatic increase in the ability for adversaries to access our net-

The Cebrowski Institute initiated a new project/capability called NEMESIS which will be a fully reconfigurable mobile computer network attack/defense and exploitation and research platform. As a part of this effort the Global Information Grid Applications (GIGA) Lab was enhanced to provide data analysis and modeling and simulation support for the mobile van.

works without physical connections and without ever being detected. Wireless communications (such as cellular telephones, cordless phones and wireless computer networks) are among some of the easiest of eavesdropping targets. Given the right conditions, motivations and resources, interception and exploitation of these wireless data transmission types are deadly "low hanging fruit" for adversaries. Cellular communications can be intercepted over hundreds of square miles

while wireless can be intercepted several miles away. In addition to being an espionage and information warfare windfall by professional adversaries, monitoring and exploitation of these transmissions has also become a favorite target of opportunistic hobbyists. This new threat must be assessed. Methods for constant monitoring of such wireless vulnerabilities must be identified and then these vulnerabilities must be remedied. The Nemesis platform is a mobile lab that

--continued on page 4



THE NEMESIS PROJECT: CONCEPT OF OPERATIONS, *continued from page 3*

will be able to provide research, training and practical experience for identification of vulnerabilities whether on a military base, ship or squadron, Federal Government installation, or critical national infrastructure civilian organization facility.

Adversaries can set up a permanent or long-term wireless attack capability in an apartment across the street from a base, ship or building completely undetected with only a few hundred dollars worth of hardware and software. Adversaries can “drive-by” or “fly-by” a base, ship or building and attack networks also without detection. The Nemesis platform will be equipped with hardware, software and antennas to identify such vulnerabilities in support of Homeland Defense and the Global War on Terrorism.

Scope

The initial concept-of-operations for the Nemesis Project will:

- Provide a requirements analysis, modeling, development and deployment of a fully re-configurable mobile computer network attack/defense and exploitation lab. This analysis has been completed.
- Create and implement a Computer Network Vulnerability Assessment Training Package via a secure website on the SIPRNET for USPACOM and other DoD organizations.
- Implement a test bed for NPS students to become familiar with emerging wireless technology vulnerabilities and adversary techniques in this area.
- Provide real-world experience for NPS students and faculty to conduct network warfare operations to include computer network attack/defense and exploitation of DoD, local, state, and federal government computer networks.
- Create experience opportunities for NPS students to generate vulnerability reports to include recommended actions by agencies that are found to be susceptible to such network attacks.
- Participate in the NPS '03 Cebrowski Institute Symposium to showcase the mobile network warfare platform and identify additional research projects/sponsors in this field of study.
- Draft Wireless network policy and deployment guidelines.
- Comment on DoD's draft wireless network policy doctrine. This task has been completed.
- Provide a legal analysis and recommendations for legally conducting wireless network vulnerability assessments. (This task has been completed.)

The Initial implementation is for western United States, but the NetWarVan could be transportable outside CONUS. In addition, a portable mobile equipment suite is planned for integration into the Nemesis Program in FY03.

The “Nemesis Project” team will successfully prove the utility of the mobile deployment platform within the virtual battlespace and will continue to provide a flexible, sustainable mobile capability to test new security applications or to identify new security vulnerabilities and weaknesses within DoD, intelligence and law enforcement communities in support of overall homeland defense.

Conceptual Model

Based on preliminary research on the ideal vehicle type, NPS is in the process of acquiring a Class 'A' Motor Coach, 1995 model, 33 feet in length, with a 7 kW generator. The vehicle's back end will be converted into a lab and work area immediately, and will have front/rear air conditioning. Part of the vehicle's main area will be also converted to a work area. The Nemesis team investigated other types of vehicle including step vans, conversion vans, and cargo vans. The team determined that the cost and time to convert such vehicles to our needs (with a network warfare lab, living spaces, generators, air conditioners, etc.) would be unreasonable.

The initial Nemesis lab and communications center consists of six laptops, a basic network server, two equipment enclosures (racks), a color ink jet printer, a laser b/w printer, an Iridium satellite phone, a Voice Over IP (VOIP) phone, an uninterruptible power supply (UPS), a mobile auto-tracking KVH 400 kbps broadband satellite Internet access system, a lightning arrestor, a KVA system (keyboard, mouse, monitor controller switch), multiple antennas for network attacks, one Yellowjacket IPAC PDA with antennas for hand-carrying to some sites, five external 120 GB hard drives (to store large quantities of log files), several 802.11 wireless PCMCIA cards, two special outdoor high performance bi-directional antennas, antenna amplifiers, and furniture for the network center.

Conclusion

Collaborative Research Opportunities of the Nemesis platform are to provide:

- Development of new knowledge, features, capabilities, and functionality in support of Homeland Defense and Net-

--continued on page 5

THE NEMESIS PROJECT: CONCEPT OF OPERATIONS, *continued from page 4*

work Centric Warfare.

- Operation of mobile state-of-the-art wireless local area network (WLAN) sub-nets in conjunction with the re-configurable intrusion detection laboratory research (RIDLR) facility located on the Naval Postgraduate School campus. We envision the RIDLR lab to function as an autonomous test bed facility to test/configure Nemesis equipment.

- Ability to function as a re-configurable networked Internet connected target or training platform for COMNAVNETWARCOM, FIWC, NIWA, USPACOM, SPAWAR, NSA, and other Blue/Red Teams.

Operational research scenarios are planned as part of the CDTEMS Fleet Transit Program with the Commander Third Fleet and the Bremerton Naval Shipyard. NPS Nemesis students are also participating with the U.S. Pacific Command (USPACOM) Computer Network Vulnerability Team (CNVT) to conduct wired and wireless network vulnerability activities in the Pacific Area of Responsibility (AOR), to include work in 802.11 wireless vulnerability assessments. The USPACOM CNVT initiative enables NPS students to accompany USPACOM CNVT staff on actual missions so that NPS students can obtain thesis ideas, and to provide valuable up-to-date hands-on education and training and assist with application of various resources (hacker tools and techniques, etc.) to the CNVT groups...and vice versa...for various types of computer network vulnerabilities. Involvement by these USPACOM-CNVT-NPS students in

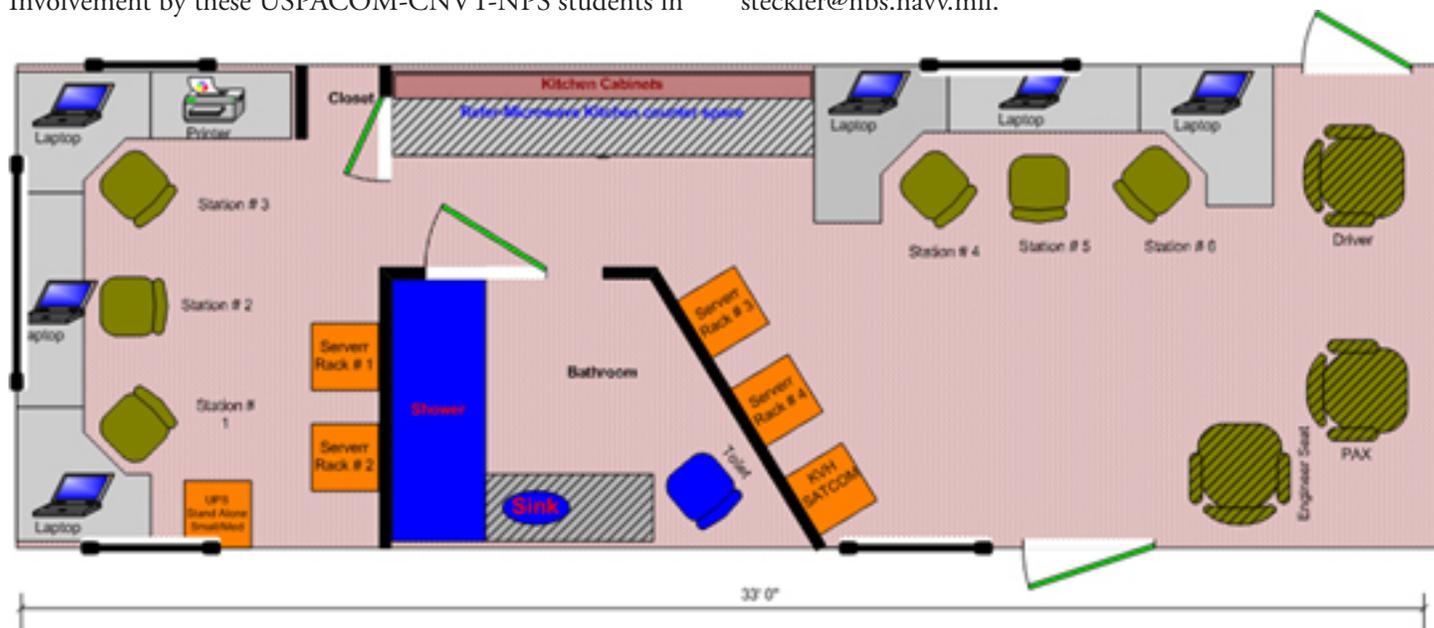
the Nemesis program will provide these students with valuable experience and training that will be beneficial for their CNVT endeavors.

The Nemesis Project is interdisciplinary, novel, and useful. Nemesis crosses several disciplines ranging from information warfare, computer network vulnerability, computer network attack/defense, information operations, electronic warfare, voice and data based telecommunications, Internet data communications, mobile research and development, and several other disciplines.

We are already collaborating on this initiative with Commander Third Fleet (C3F) as well as HQ US Pacific Command (USPACOM). NIWA and FIWC have also expressed interest in this work. We envision much broader interest and support, as virtually every company, ship, squadron, shore command, and federal/state government entity are susceptible to this new and rapidly developing field of study – and threat.

We recognize that NSA, the FBI and other state and federal agencies have been in the signals intelligence (SIGINT) and signals exploitation business for many years. However, the objectives of this initiative complement rather than compete with such operations.

NPS and the Cebrowski Institute encourage those who might be interested in collaborating with the Nemesis Team and/or utilizing its capabilities to contact Brian Steckler at steckler@nps.navy.mil.



NetWarVan Layout Diagram - Proposed Design/Layout by Maj Timothy D. Kornacki, USMC.

NETWORK MANAGEMENT FOR UBIQUITOUS SURVEILLANCE ENVIRONMENT

LtCol D. Overton, United States Marine Corps
 LtCol C. Ahciarliu, Romanian Air Force
 Maj Brandon Johnson, United States Marine Corps
 Associate Professor Alex Bordetsky, Department of Information Science

Introduction

This project is a component of a larger body of research involving the Nemesis Van and thesis research in the area of Ubiquitous Surveillance. The objective is to develop a small but architecturally representative testbed to demonstrate a limited set of capabilities inherent in a ubiquitous surveillance network, with a focus on the network management aspects of such.

The testbed developed for this project provided some limited details about network management which are reported in this paper. Much of the added value of this examination comes from the extrapolation of this information into the operational scenario, and particularly a more robust and expanded network. The discussions that follow, therefore, each have two components; the empirical findings that are limited to the experimental environment and the extrapolated assessments based on the expected or defined operating environment and configuration for this system.

Application and Network Operation Scenario

While the definition of “ubiquitous surveillance” is open to some interpretation it is defined in this paper within the context of a scenario that limits its scope to a particular notional architecture. Additionally, it is conceived that a “ubiquitous surveillance” network or system would be part of a DoD capability that is linkable to the Nemesis network operations center.

Scenario/Notional Network Construct

A ubiquitous surveillance system would be comprised of a network of multiple sensors that are potentially of multiple types (e.g. chemical, biological, nuclear, seismic, radar, IR, electro-optical, acoustic, etc.). These sensors are connected to a node (notionally a computer, but perhaps in the future a purpose built device) and collectively they monitor a particular, limited geographic area. In a deployed scenario, there would likely be multiple nodes (network elements), covering multiple limited geographic

The CDTEMS Program provides support for the Global Information Grid Applications (GIGA) Lab. The GIGA Lab provides: 1) a network operating center for the NEMESIS Project which mirrors and complements the wireless network operations at the mobile site of the NEMESIS van; and 2) long-term network management data analysis and modeling and simulation support for Information Operations.

areas, feeding into a central monitoring and/or command environment (ubiquitous surveillance network operations center (NOC)). For the purposes of this project, the central monitoring or command node is envisioned as being collocated on the Nemesis van.

The majority of these sensors would be organizationally organic equipment as their interface, management, and integrity would need to be guaranteed. This would not preclude the inclusion of potentially trusted second party sensors as long as their status as such was known (e.g. tying in to allied forces camera network). A notional diagram of the diversity of sensors and their connections is shown in Figure 1.

--continued on page 7

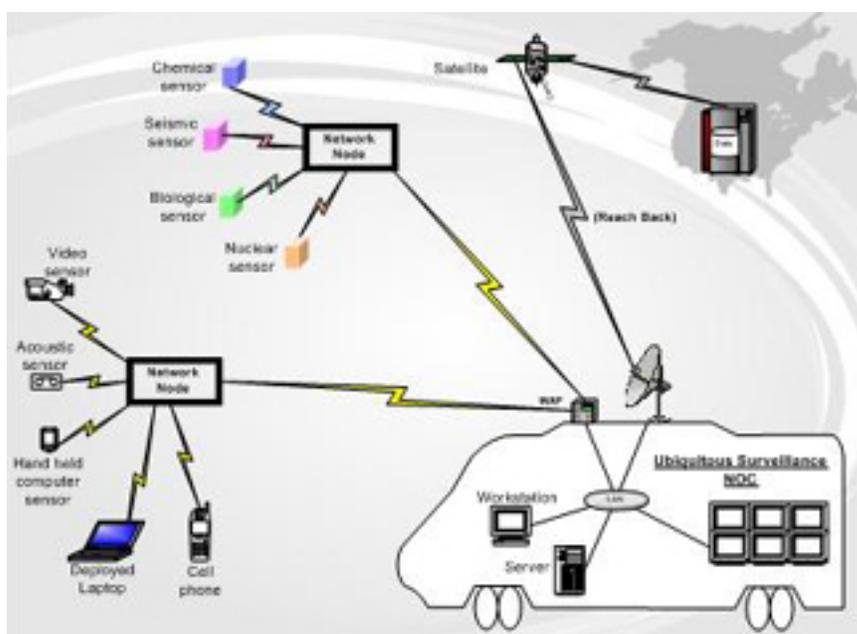


Figure 1. A notional diagram of the diversity of sensors and their connections.

NETWORK MANAGEMENT FOR UBIQUITOUS SURVEILLANCE ENVIRONMENT, *continued from page 6*

Configuration of Managed Network

The notional network defined in the scenario above reasonably demonstrates the diversity of the physical configuration of a deployed sensor network. Obviously, reproducing this in a lab environment with the limited time and resources available was not possible, nor necessarily desirable.

The intent of this project was to lay the groundwork for further experimentation and research by modeling a small portion of the network architecture. It was determined that minimum requirements included a mobile (or potentially mobile) node, a real-time sensor feed, network management software (NMS), a fixed node, and representative sensor application software. The actual components and configuration of the testbed are listed below.

Physical

- Fixed node: Dell Dimension 4500 desktop workstation - representing the server station connected to NPS network using a wireless card. Although it is a fixed piece of equipment, in a larger scenario it would represent the mobile NOC of the Nemesis Van.
- Mobile node: Dell Inspiron 4100 laptop - representing the mobile client. This simulates to a small degree the mobility and wireless factors of the nodes attached to the Nemesis Van.
- Sensor: Logitech, Quickcam Pro 4000, digital camera, (NTSC format), USB connection.

Software

- Network Management Software: Solarwinds Engineer's Edition (Hewlett Packard).
- Sensor Application Software: ID-2000 (Imagis Technologies Inc.)
- Windows XP Professional (Microsoft)

A model of the testbed is shown in Figure 2.

Link: In the deployed ubiquitous surveillance scenario, the link layer (or layer 2 of the open systems interconnect (OSI) network model) takes on increased importance. This is primarily due to the heterogeneous mixture of network elements in the network, many of which are wirelessly connected and therefore more susceptible to degradation due to environmental or intentional interference. Heterogeneity is a factor because not all sensors require the same perfor-

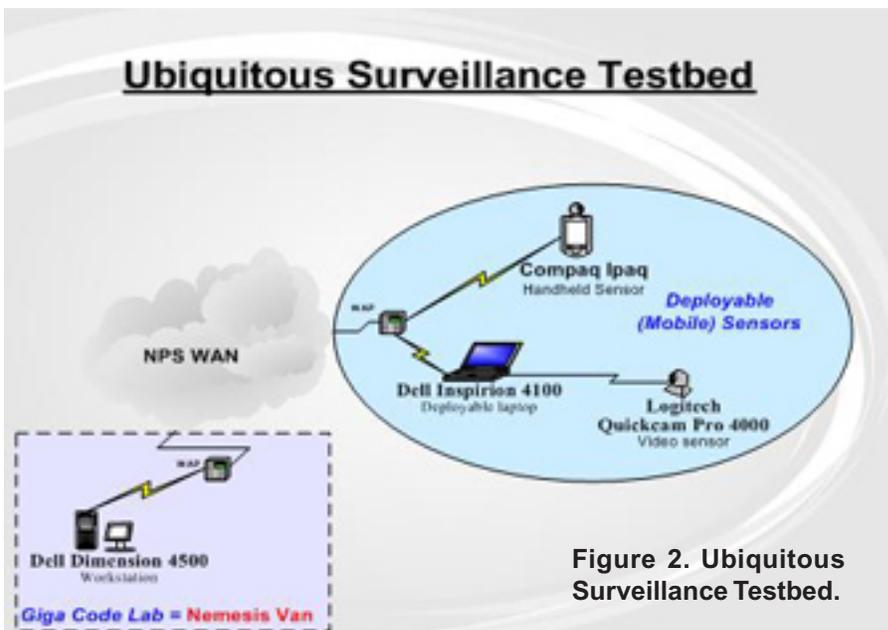


Figure 2. Ubiquitous Surveillance Testbed.

mance parameters, and therefore the network management software will need to use different management information base (MIB) variables and metrics to determine whether a particular link is operating correctly. Obviously, knowledge of link status is critical, as there will likely be a requirement to know when a particular sensor is unable to communicate effectively with the network because of a degraded link.

It was intended to model a possible degraded link in the testbed environment by ensuring that the two primary nodes communicated with each other via wireless access points. This would offer the opportunity to examine the effects on a degraded link as conditions changed (e.g. the laptop was carried down the hall).

Networking: Based on the platforms being used, and the network that they are connected to, the internet protocol (IP) is the primary layer 3 service employed by the testbed. There are other services riding on IP (TCP, SNMP, etc.) that are needed to enable the application being tested in this experiment, as well as facilitate the NMS (SolarWinds).

Application:

- Description of ID-2000. ID-2000 allows the recording and matching of facial images. It uses a 3-dimensional deformable surface model that it fits to the subject being imaged by making deformations to fit the face. These deformations are refined many times, closely matching the features of the face being imaged, and the results of the deformations

--continued on page 45

INTEGRATED ASYMMETRIC GOAL ORGANIZATION (IAGO): A MULTI-AGENT MODEL OF CONCEPTUAL BLENDING

Research Associate Curt Blais, The Modeling, Virtual Environments, and Simulation Institute

Research Professor John Hiles, The Modeling, Virtual Environments, and Simulation Institute

Professor Ted Lewis, Department of Computer Science

Bruce Allen, Digital Consulting Service

Neal Elzenga, Emergent Design

Gary Ackerman, Monterey Institute of International Studies

Background

Thomas C. Schelling, in his forward to the definitive book about why we were surprised at Pearl Harbor, describes the inability of governments to anticipate effectively:

The danger is not that we shall read the signals and indicators with too little skill; the danger is in a poverty of expectations – a routine obsession with a few dangers that may be familiar rather than likely. Alliance diplomacy, inter-service bargaining, appropriate hearings and public discussion all seem to need to focus on a few vivid and oversimplified dangers. The planner should think in subtler and more variegated terms and allow for a wider range of contingencies. But the same people who need to think in extended ways are the ones who have the most to do during a crisis. This project explores the question of whether or not software, in the form of a computational model of cognitive behavior, can contribute to better anticipation of asymmetric threats.

Current technical solutions that attempt to help in anticipation are usually based on rational choice models. In a rational choice model, the designer produces a set of alternatives that may achieve some goal. Each of the alternatives is equipped with a utility function. The utility function produces a number that represents the Effective Utility of that option (i.e., the product of the probability that the alternative will work times the value or result if it does work). Rational choice models have two limitations that are particularly important in connection with anticipating asymmetric conflict. The first limitation is that rational choice models assume the subjects will always be purely rational. The second limitation is actually more important; it involves the important relationship between innovation and asymmetric conflict. In a rational choice model the alternatives have to be constructed along with their utility functions by a designer. The model designer's assumptions limit the options that the subject of the model can choose. But an asymmetric conflict the innovations of the subject are often the most important dimension of the analysis. As we will show later in this paper,

In the MOVES Institute, a new center was formed -- the Center for the Study of Potential Outcomes. Its initial project focused on a multiagent model of conceptual blending in which agent technology can create new knowledge based on its experience and processing. The goal is to provide a computational model which can contribute to better anticipation of asymmetric threats such as terrorist behavior.

the IAGO project proposes a model in which innovation is an intrinsic part of the behavior of the software model. The subject model constructs new options as it goes. That it is a key part of IAGO and an important distinction with traditional rational choice models.

Our approach focuses on the cognitive foundation of the subject – what things mean to the subject. Clinical psychiatry tells us that the understanding of what things mean to the subject is the key to understanding the subject's behavior, the cognitive context of the subject's actions. It is clear from the clinical experience with individuals who are pre-disposed to violent activity that events have very different meaning to these subjects. In most cases, the person that we see committing the violent action perceives himself to be a victim and perceives that the target of the violence is at fault and in many cases is the cause of the problem.

One of the key developments in cognitive psychology over the last decade has been a model that proposes mental spaces and conceptual blending as the mechanisms for conceptual integration or the construction of meaning. With the help of this model, it is possible to explain the process by which a subject constructs new knowledge and meaning from a stream of events. And that is precisely what we would like the software in our model do in order to help us with the anticipation of subject behavior.

Our multi-agent work at Naval Postgraduate School has produced a number of new techniques over the last three years that will help us to implement this conceptual blending and mental space model. We have defined Tickets to serve as packages that incorporate knowledge inside an agent. Connectors coordinate the activities of multiple agents. We have extended the connector idea so that when two agents form a connection, the connection can become persistent, resulting

--continued on page 9

INTEGRATED ASYMMETRIC GOAL ORGANIZATION, *continued from page 8*

in a scale-free network that is based on the coordinated behavior of the agents. So we can use our agents to produce a “bottom-up” emerging behavior. Then, as the agents make connections and coordinate with each other, the resulting structure allows us to create very complicated emerging behavior. A project completed in 2002 demonstrated the large-scale use of tickets and connectors.

In IAGO we combined these techniques to do conceptual blending with software.

Research Objective

The key assumption behind IAGO is that the context of meaning in a subject is the key to understanding and anticipating the subject’s behavior. In other words,

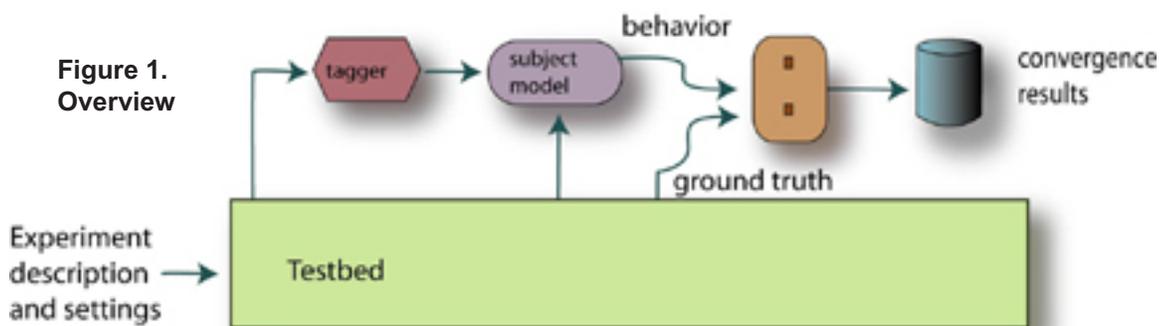
IAGO is interested in shifting the attention from the point of view of an observer to the perspective of the subject. Key events arrive as inputs to the subject, where a perceptual filter applies meaning to the events, which are then incorporated into the subject’s

mental apparatus. By using a computational model of blending, IAGO will attempt to construct blended mental spaces that represent new meaning or context of cognitive behavior. In this way, IAGO takes a bottom-up approach. The multi-agent system will continually adjust the relationships of mental spaces represented by agents to form structures that fit the context of the subject and, as the subject changes because of learning and actions, the structure of the multi-agent system will also change. This may be the single most important advantage of the multi-agent approach to simulation. The continuous goal-oriented adaptation of the system’s structure -- when multi-agent systems modify their structure based on the goals and intent and the adaptation of the individual agents. Compared to other software systems, this connection between modification of structure and goal-orientation is the key to understanding a multi-agent system. This goal orientation of the software creates the autonomous behavior of the agents, and it is the modification of the multi-agent system structure based on goal orientation that allows

and supports complex behavior. The complex behavior is represented by the modified structure. Continuous adjustments to structure support the production of evolving complex behavior and that allows us to explore the cognitive patterns in the subject.

The motivation behind IAGO and the ultimate goal for the project is a blending multi-agent system driven by tagged input streams produced by subject-matter experts. The overview illustration of IAGO explains our approach.

The project subject matter expert has created a body of information that was known to the subject. This information is tagged with type information and is time-stamped according to when the information reached the subject. A further refinement in our system allows us to limit the input



information according to the certainty attached to it. For example, once this element of the system is implemented, we could limit a run to only information that was known to reach the subject as a certainty. Or we could do a run that combined very concrete input with some very reasonable inferences about input. Thus, the project would have a control over the degree of speculation that was involved in the input stream reaching the subject. In future implementation it would be possible to extend this concept and permit hypothetical events to be fed into the stream so that observers can watch the behavior of the subject model. As tagged information reaches the subject model, blenders combine the input mental spaces to form new blends. Our goal is to have these blends formed very fast and very smoothly and constructively. Cognitive psychologists point out that blending goes on continuously, it is very fast and that we are seldom aware of the blends that we’re constructing. As blends are produced in the subject model, they return to the blender to

--continued on page 10

INTEGRATED ASYMMETRIC GOAL ORGANIZATION, *continued from page 9*

receive further processing.

As more and more of the interior of a blend are filled out with subsequent blending, the blended plan approaches a point where all of its pieces are in place. At this point, the blend is ready to actuate behavior. The completed blend moves to an output part of the agent where it is emitted into the comparator part of the test bin. The comparator captures the behavior and makes it possible to compare with the ground truth events that describe the subject's behavior based on the subject matter expert's research.

The first step for IAGO was to produce an example of software blending that uses hand tagged subject matter expert inputs based on research into the subject and to demonstrate that the model outcomes,

Figure 2. Subject Model (Composite Cognitive Agent).

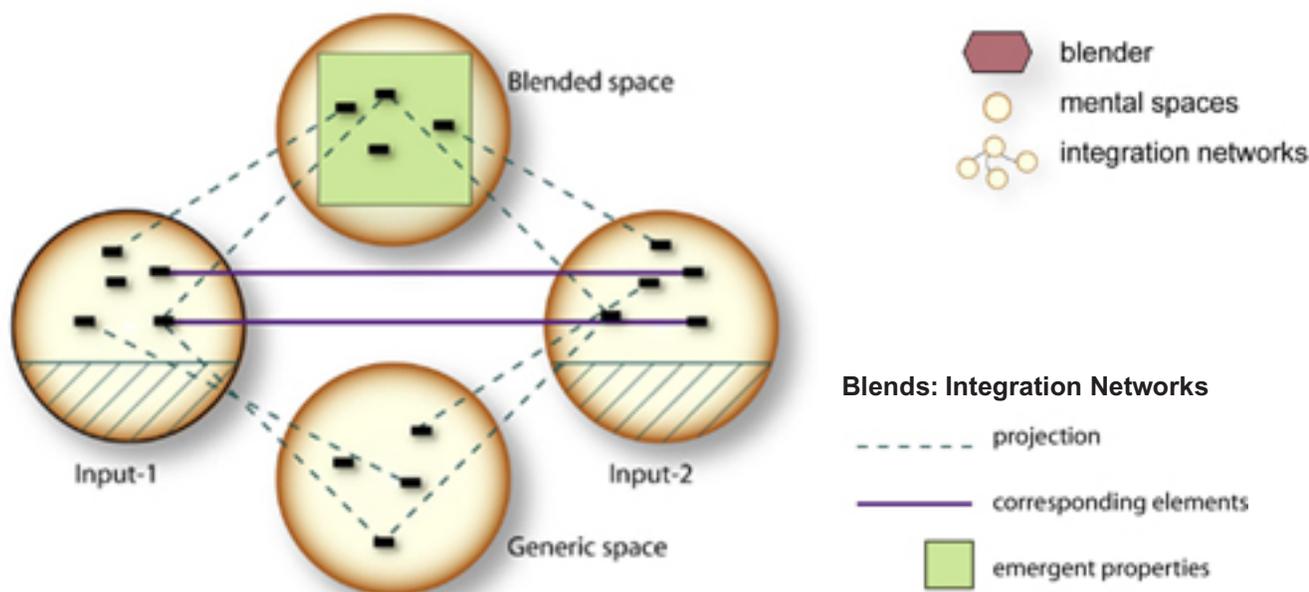


although they may include a variety of paths, include the behavior that was revealed in the ground truth.

In the blending model, we see mental spaces coming together and forming what the cognitive psychologist calls integration networks.

In an integration network we have two input mental spaces. These form on either side of the blender. Associated

--continued on page 11



INTEGRATED ASYMMETRIC GOAL ORGANIZATION, *continued from page 10*

with the two input mental spaces is the mental space called the generic space. It comes up from the bottom and attaches to the blender. The generic space contains type information, process information and techniques for projecting information elements from the two inputs into the new blended space at the top. The blended space will contain information found in the two input spaces but also new information not present in either one of the input spaces. This can take the simple form of a combination not found in either one of the input spaces or more complicated forms that involve fusing or compression of information. When the blend is completed as determined by the generic space, the mental spaces leave the blender. But the connections that have held the mental spaces to the blender are converted into persistent links to form the new integration network with the blend at the top, the two input spaces and the generic space connected as a network. The new blend can return to a blender and be used in subsequent blends. Upon each return to a blender, new links are formed in the shape of a growing integration network. These networks satisfy the properties of a scale-free network in that the links are formed preferentially and incrementally.

If we look at a closer view of blending, we will see that the frames of a mental space serve as a recipe for that type of mental space. For example, in our project we have an attack plan that is one type of generic space. When we examine an attack plan, we can see the generalized concept – the concept of generalized components. So, an attack plan is made up of the following pieces: a target, a harm-agent, an exit route, an optional exit route, a trigger and a symbolic value. Each of the 40 to 50 types of generic spaces was constructed with the help of our subject-matter expert, and each of them has this type of internal structure highly generalized. These generic spaces are what guide the formation of new blends.

The central features of blending include the fol-

lowing properties: cross-space mapping, partial projection from inputs, generic space, integration of events, and emergent structure. Cross-spaced mapping means that information elements in the two input spaces are connected because they involve the same type of information. Partial projection from the inputs is guided by the generic space. Not all of the information in the two inputs is going to make it into the blend. Selected information is pushed up to the blend. Different combinations are tried; feedback is used to decide where the blends are effective or not effective. Generic spaces contain the meta-data that guides the projection and compression operations that result in a new blend. Emergent structure is a key to the success of blends. The information found in input 1 or input 2 can be projected selectively, can be fused or compressed by the generic space. The result is that the information that ends up in the blend is not the same as the information in either of the inputs. Something new has emerged in the process of blending. The software blender itself is an agent-based device, an illustration that shows a

--continued on page 18

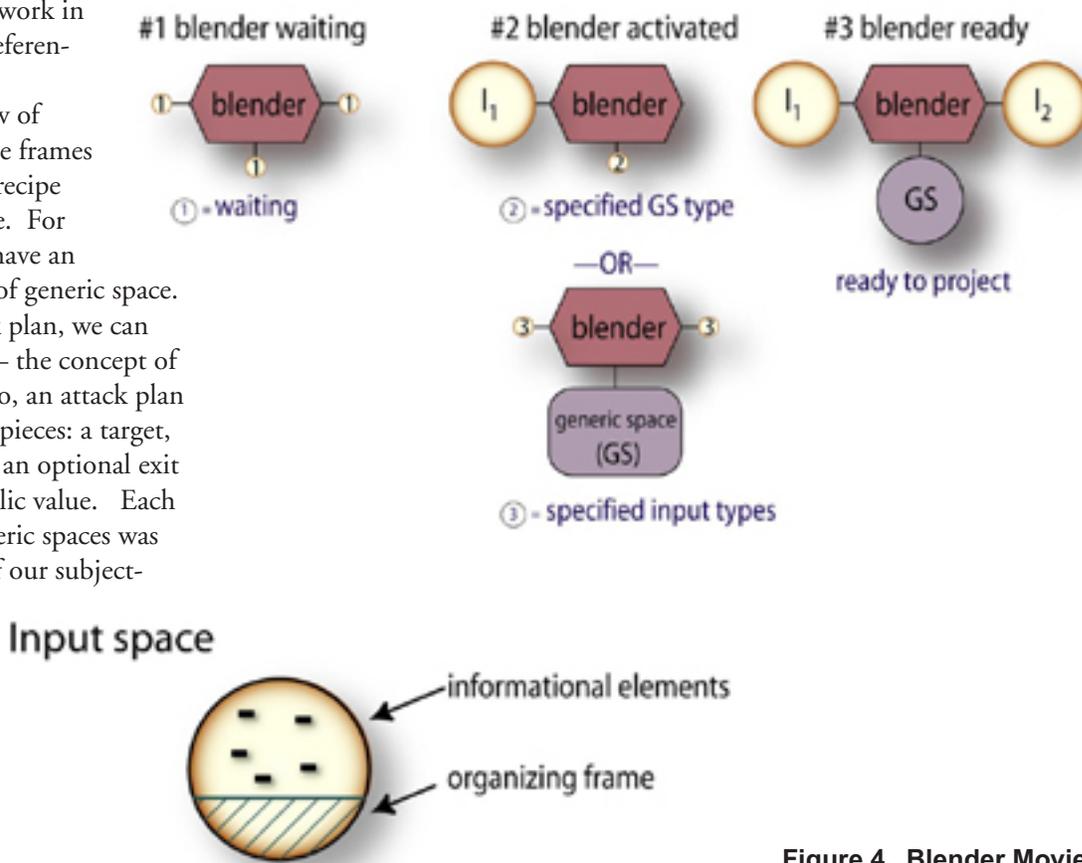


Figure 4. Blender Movie.

INTEGRATED PROJECT IN EXPEDITIONARY WARFARE COMPLETE MAJOR MILESTONE

The Wayne E. Meyer Institute of Systems Engineering (Meyer Institute), one of three Institutes on campus, has as a major objective the identification of significant defense problems that could potentially benefit from an interdisciplinary search for solutions. In addition to its educational and research interests, the Institute actively seeks such important, broad problems, with a view toward assembling a project team of faculty and students who can employ Systems Engineering methods to promote understanding of the problem and provide insights to decision makers.

The Institute's first major campus integrated project of this type is a system of systems exploration of Expeditionary Warfare. Phase one of the planned two-year effort completed in December 2002, with follow on work to continue into 2003. The Meyer Institute is guided by a Board of Advisors chaired by OPNAV N7, the Deputy CNO for Warfare

The Meyer Institute (MI) provides unique graduate education and research to increase the knowledge and skills of military officers and the supporting civilian force in systems engineering, systems analysis, and large-scale experimentation. In addition to applied research in these areas, this Institute sponsors a campus-wide interdisciplinary systems engineering project that addresses force-level issues. The MI year-long student project was a system of systems review of Expeditionary Warfare.

Requirements and Programs (VADM Dennis McGinn at the time of the project) who approve the tasking. The Director of the Expeditionary Warfare Division, OPNAV 75, acted as the project sponsor. The faculty leadership of the study was provided by the Meyer Institute, with **Professor Charles Calvano**, the Meyer Institute Technical Director, serving as the overall coordinator. A total of over 70 students and approximately 18 faculty members from numerous campus organizations participated (see Table 1).

Officer students from the Systems Engineering and Analysis (SEA) program played the role of overall project Systems Engineers, while students in design projects courses in the Aeronautical Engineering program, the Total Ship Systems Engineering (TSSE) program, and others performed portions of the overall design task.

Officer students enrolled in the SEA program are educated in how the Navy builds and operates large combat systems of systems. The primary objective is to prepare them to serve in operational billets by giving them the technological and analytical understanding to fight today and in the future. The emphasis is on analysis and integration of complex warfare systems with compatible tactics. In addition, graduates with experience afloat are prepared to serve ashore as program managers and in technical/analytical billets on headquarters staffs. Systems engineering of a major project, as a team, is an integral part of their curriculum.

The OPNAV tasking directed NPS to use a top down, system of systems approach to examine future Expeditionary Warfare operations in terms of current and emerging operational concepts. Of major interest was the emerging concept of Seabasing to support the Marine Corps' doctrine of Ship-To-Objective-Maneuver (STOM).

Table 1. PARTICIPATING FACULTY

- Chuck Calvano (Meyer Institute, Mechanical Engineering, Systems Engineering)
- Dave Olwell (Operations Research, Systems Engineering)
- Wayne Hughes (Graduate School of Operational and Information Sciences)
- John Osmundson (Information Science)
- Bob Wood (Aeronautics and Astronautics)
- Chip Franck (Systems Engineering)
- Dave Schrady (Operations Research)
- Bob Harney (Systems Engineering)
- Fotis Papoulias (Mechanical Engineering)
- CAPT Jeff Kline, USN (Meyer Institute, Operations Research)
- CDR Mark Rhoades, USN (Aeronautics and Astronautics)
- Bill Kemple (Information Science)
- Russ Duren (Aeronautics and Astronautics)
- CDR Mark Couch, USN (Aeronautics and Astronautics)
- Dan Boger (Information Science)
- Barry Leonard (Aeronautics and Astronautics)
- Phil Depoy (Meyer's Institute)
- LCDR Russ Gottfried, USN (Operations Research)
- Lee Edwards (Graduate School of Business and Public Policy)

--continued on page 13

INTEGRATED PROJECT IN EXPEDITIONARY WARFARE, *continued from page 12*

The team decided to employ both a Top Down and Bottom Up approach. The Top Down approach examined current and proposed operational concepts such as STOM and Sea Basing. The SEA students performed a Functional Analysis of the Expeditionary Warfare mission using Functional Flow Block Diagrams and Integrated Definition Language notation to define the **capabilities required** to perform Expeditionary Warfare. In order to determine the **capabilities actually expected to be available** for Expeditionary Warfare, the Bottom Up approach examined the current and planned Navy and Marine Corps expeditionary force architectures, referred to in the tasking as the “programs of record.”

The team identified capability gaps by comparing the **capabilities available and the capabilities required** (Table 2). Once these gaps had been defined and prioritized, they allocated the most important of them to platform solutions. The team generated conceptual design requirements for a family of ships capable of supporting STOM operations through a Sea Base; a long range, heavy lift aircraft; and a multi-tiered family of intelligence, surveillance, and reconnaissance (ISR)

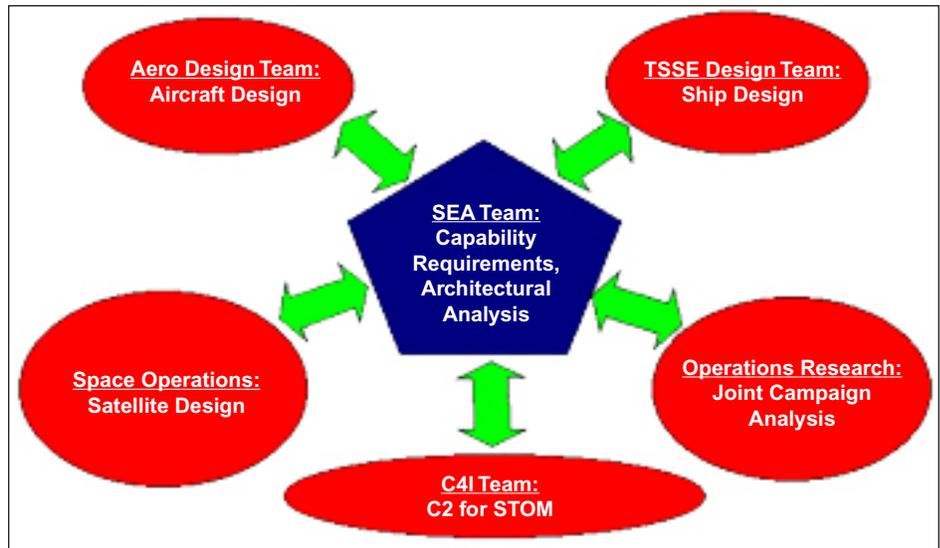


Figure 1. Integrated Project Design Teams.

systems to various supporting NPS design teams as shown previously in Figure 1. The ultimate result was a conceptual architecture; a mixture of planned and conceptual platforms designed to be capable of fully implementing the Ship to Objective Maneuver and Sea Basing doctrines.

To compare the performance of the conceptual architecture against the current and planned architectures, the team generated a large scale, high resolution dynamic model capable of tracking personnel, vehicle, and material flows from CONUS through the Sea Base and on to the Objective at the level of the individual Marine, vehicle, and supply commodity. They compared the three architectures' abilities to project combat power ashore and determined the effects of weather, mine warfare, distance to the objective, and personnel and vehicle attrition on the ability to execute an expeditionary operation.

The metric used was Combat Power Ashore, which is the sum of Combat Power Indices assigned to individual Marines, combat vehicles, and artillery pieces placed at the objective. The fitness of each architecture was measured by the time required to place combat power at the objective under the influence of the four previously mentioned factors. The analysis used two measures of performance: the Time to Build Up Advanced Force (TAF), which represented the time to insert one company of infantry and supporting equipment at the objective and Time to Build Up Desired Force Level (TBU), which represented the time required to place 80%

--continued on page 14

Table 2. CAPABILITY GAPS IDENTIFIED

- Surface Platforms Capable of Forming and Sustaining a Sea Base
- Shipboard Aircraft Capable of Transporting Large Loads Over Long Distances
- Ability to Rapidly Deliver Combat Force to Theater
- Highly Survivable Air Transport Platforms to Sustain STOM Operations
- Organic Capability to Collect ISR Data throughout Area of Operations
- Ability to Support Marines Ashore with Both Precision and Volume Fires from the Sea Base
- Ability to Provide Sufficient C4 Support to Fully Implement STOM
- Providing Force Protection for Surface Craft Transiting to Shore
- Robust Organic Mine Countermeasures Capability

INTEGRATED PROJECT IN EXPEDITIONARY WARFARE, *continued from page 13*

of a Marine Expeditionary Warfare (MEB) sized Ground Combat Element and its supporting equipment at the objective. The sustainment measure of performance was the mean square error in days of supply at a particular location, which represented a deviation from a desired level of supply. Some of the major conclusions included:

- The Time to Build Up the Advance Force (TAF) for each architecture was insensitive to the effects of weather, mines, and distance from the objective.
- The proximity of the ships to the objective and weather conditions are the main influences on the Time to Build Up to the Desired Force Level (TBU).
- Under good weather conditions, commencing the MEB assault from a greater distance at sea does not increase TBU significantly.
- Improved aircraft combat survivability (through threat suppression, use of escort aircraft and/or more survivable aircraft designs) is critical for successful sustainment of the objective in STOM operations.
- The Current Architecture, with the accompanying “Iron Mountain” of logistic support ashore, takes the longest time to build up forces ashore and is the most robust in sustaining the objective. The operational commander must be willing to accept the accompanying operational pause and the potential vulnerability of the “Iron Mountain.”
- With Current and Planned Architectures, Sea Basing appears to be a viable operational concept, but only under good weather conditions.
- Under all conditions, the Conceptual Architecture was able to project forces ashore in the shortest time, since its increased number of MV-22 and conceptual long range, heavy lift air assets were better able to project forces up to the 275 nm from the Sea Base required by doctrine.
- The longer transport ranges and larger number of aircraft required make the supply of fuel a more critical concern.
- While large numbers of aircraft are required to implement STOM and re-supply from a Sea Base over the long distances envisioned in the doctrine, there remains a need to retain an effective surface craft transport capability to project high volume and weight loads, such as the M1A1 tank, ashore.

The N7 tasking also requested the examination of several excursions; the most significant of which involved the effects of speed and the impact of High Speed Vehicle (HSV) platforms on Expeditionary Warfare. The team examined a Joint Venture class HSV as an alternative to a Fast Support

Ship large bulk cargo ship and determined that at its current cost, speed, and payload, the HSV was not an effective replacement for an FSS to resupply the Sea Base. The HSV, however, shows significant promise for other than logistics-resupply functions – such as force protection or mine warfare.

The tasking also requested an analysis of the impact of reduced footprint ashore. The team’s analysis showed the most significant factors in reducing footprint were the air transportability of supplies and increased reliability of equipment.

This study was an academic exercise and its results have not been endorsed by either the Navy or the Marine Corps. The scenarios used were created purely to facilitate our analysis and do not represent the official views or policy of the Navy, Marine Corps, or any government.

Because of time constraints, the study did not examine all of the capability gaps identified. For example, the team did not conduct an analysis of the costs and benefits of, or the design of systems for, providing precision and volume fire support from the Sea Base. They also did not conduct a detailed examination of C4ISR systems and their requirements to support STOM nor did they conduct analysis of more detailed operational concepts such as “Sense and Respond Logistics” and “Enhanced Networked Sea Basing.”

The initial tasking, to examine Expeditionary Warfare in its entirety, was extremely challenging, since virtually any military activity can be relevant. It was obvious from the start that the teams could not cover all elements of Expeditionary Warfare in depth. Despite the need to curtail some aspects of the inquiry, the study produced results useful to our sponsor and our methodology provides a jumping off point for additional paths of inquiry.

A daylong series of presentations of the study results was given at NPS on 5 December, with approximately 100 visitors from government and industry in attendance. Post-presentation discussion sessions provided the opportunity for feedback and the exchange of ideas. Plans for the second phase of the study will be developed during the winter quarter (January-March) of 2003.

The materials from the 5 December presentations and an executive summary of the study report are available online at www.nps.navy.mil/sea/exwar. The full report will be made available as requested.

INFORMATION OPERATIONS SUMMER STUDY

Center on Terrorism and Irregular Warfare
Associate Professor David Tucker, Director

The Center on Terrorism and Irregular Warfare received CDTEMS funding in FY 02 to analyze requirements for education in Information Operations (IO). This research was done for the Office of the Deputy Assistant Secretary of Defense for Resources and Plans and the Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence.

The purpose of the research was to devise options for an expanded and integrated educational program in IO to support an IO career force. The research had three components: a requirements conference; a database of existing IO courses; and a research seminar at NPS.

The critical task of the research was to assess the difference between what the DoD educational system currently offers and what it will need to offer in order to support a career IO force. The research accomplished this task by comparing the database of current educational offerings with the requirements established at the conference. In addition, the research seminar looked at the fields currently identified as the components of IO (computer network operations, electronic warfare, psychological operations, deception and operational security) to see how they constitute an integrated activity called information operations. The seminar examined both the five components of IO and the concept of IO itself in order to make sure that the educational program in IO is integrated and comprehensive. Finally, based on questions raised during the research, the researchers also addressed the relationship between public affairs and psychological operations.

The recommendations developed in this summer study form part of a decision briefing that the sponsors will present to the Secretary of Defense.

Requirements Conference

The requirements conference brought together representatives from OSD, the Joint Staff, the Services and those commands and agencies that will employ the officers in the new IO career field. The conference lasted two days and consisted of briefings and work on assigned topics in small groups. Conference participants heard a brief on Joint Professional Military Education (JPME) that explained the significance of educational skill requirements, how they are derived and the general characteristics of the phases of JPME.

In FY02, CDTEMS embarked on several additional new programs, which included two summer studies and the development of a comprehensive short course which addressed a critical emerging area for the warfighter – Unmanned Aerial Vehicles.

With this briefing as preparation, the participants then heard a series of briefs by the Services, Joint and Service IO components, and the defense agencies. The briefs provided information on the IO skills that personnel need in order to function effectively in each organization. The briefs also described any educational shortfalls the organizations have noted. After the briefs on skill requirements and shortfalls, conference participants split into working groups. Each working group developed the educational skill requirements for a specific phase of JPME. The conference concluded with each working group briefing the plenary session on the educational skill requirements it has developed.

The list of educational requirements developed at the conference has subsequently guided the development of the IO education program by the OSD sponsors.

IO Course Database

Based on information provided by the Services and DoD agencies, NPS staff constructed a database of all IO courses offered in DoD. This was the first comprehensive listing of such courses. It allowed officials to have an accurate view of deficiencies that before had been known only anecdotally. Used in conjunction with the requirements derived from the conference, it has served as an important planning tool.

The database will be posted online and updated. In addition, a version will be developed as a reference tool for use by those interested in taking IO courses.

NPS Research Seminar

The research seminar included four students, who took the class for credit, the principal investigator and a cast of other students and faculty that varied according to topic. The seminar brought two nationally known figures in IO (Dorothy Denning and Martin Libicki) to NPS, as well as military officers who had directed IO on combatant command staffs and civilians who direct significant IO activities in DoD. The seminar also included presentations by several NPS faculty. In addition, the students in the seminar made presentations on research topics. Each of the students involved in the seminar decided to make these research

--continued on page 16

MONTEREY SUMMER STUDY: U.S. DEFENSE POLICY OPTIONS FOR SOUTH ASIA

Assistant Professor Peter Lavoy, Department of National Security Affairs

Objective

The aim of this project was to conduct preliminary education and research activities to prepare the ground for a possible FY03 NPS summer study on U.S. Defense Policy Options for India and Pakistan in the wake of the U.S.-led war on terrorism in Afghanistan.

Accomplishments

A plan for a future summer study was developed through discussions with: 1) U.S. policy makers (in OSD, Joint Staff, State Department, etc.) in Washington, DC; 2) U.S. country teams in U.S. embassies in India and Pakistan; and 3) Indian, Pakistan and American experts on South Asian security.

Additionally, internationally recognized authors were com-

missioned to write policy papers on the following topics:

- The role the United States should play in helping to resolve the Kashmir dispute.
- Policy options to secure and safeguard the nuclear weapons facilities and materials of
 - India and Pakistan.
 - Measures to promote deterrence stability between India and Pakistan.
 - Measures to counter terrorism in South Asia in the long term.
- Options for the pace and scope of U.S. security cooperation with India.
- Options for the pace and scope of U.S. security cooperation with Pakistan.

DESIGN, PERFORMANCE AND ANALYSIS OF UNMANNED AERIAL VEHICLE SYSTEMS SHORT-COURSE

The Naval Postgraduate School will present the Design, Performance and Analysis of Unmanned Aerial Vehicle Systems Short-Course 7-11 April 2003. This course is intended for military officers and civilians who have a technical interest in the design of Unmanned Aerial Vehicles (UAVs) and Unmanned Combat Air Vehicles (UCAVs). This program is of special significance since it concentrates on the current missions and operations as well as Measurements and Signals Intelligence (MASINT), sustainability and force effectiveness. Also included are sessions on training of UAV operators and the human factor issues of crew station design. Special emphasis is given to safety and reliability concerns. Vehicle design tradeoffs, design of the payloads and links, navigation, guidance and control for weapons delivery, and the design of UAV

antenna systems are also presented. A special plenary session will cover the evolution of the NATO Standardization Agreement (STANAG) 4586, the standard interface of unmanned control systems for NATO UAV interoperability and the key to successful coalition operations in the future.

This Short Course will provide an excellent opportunity for exchanging information on UAV and UCAV technology. A summary of the program is provided below. Registration information is available at http://ocd.nps.navy.mil/npsconferences/uav_short_course/.

- Introduction to Missions, Operations and Advanced Concept Technologies
- Introduction to Measurement and Signatures Intelligence (MASINT)

- UAV Sustainability, Force Effectiveness
- UAV System Safety and Reliability
- The "Man" in Unmanned Systems
- Vehicle Design
- Payloads and Links
- UAV design and Payload Tradeoffs
- Antenna Systems for UAVs
- Case Study in UAV Development: Global Hawk
- Navigation, Guidance and Control of UAVs for Weapons.

INFORMATION OPERATIONS SUMMER STUDY, *continued from page 15*

topics their Master's thesis topics.

The principal accomplishment of the seminar was to provide a forum in which various IO concepts developed by OSD could receive an informed and critical review. Two issues received the most attention. First, in keeping with the original intent of the research, the seminar reviewed the OSD briefing that defined IO and the relationships between its five constituent parts. From this work developed a second separate task, defining the relationship between public affairs and psychological operations.

STRATEGIC INSIGHTS

Center for Contemporary Conflict

Assistant Professor Peter Lavoy, Director

Strategic Insights (SIs) provide concise monthly analyses of regions and issues critical to U.S. national security. CDTEMS funded the Center for Contemporary Conflict to produce SIs for the Center for Contemporary Conflict and the Regional Security Education Program website. In FY02, extensive coverage of central concerns to U.S. national security, such as the War on Terrorism (19 SIs) and the conflict with Iraq (10 SIs) were provided.

The list below shows the coverage that we provided for different regions and issue areas, from 1 March through 1 October 2002. (Note that some SIs appear in more than one category.)

Middle East

- Odium of the Mesopotamia Entanglement
- Deterrence and Preemption
- China and the Iraq Question
- Comparing Threats from Saddam and bin Laden
- Deconstructing the U.S.-Saudi Partnership?
- Where is Iran Headed?
- Assessing Al Qaeda's WMD Capabilities
- Nuclear Weapons, War with Iraq, and U.S. Security Strategy in the Middle East
- Bush Enters the Middle East Fray
- WMD Proliferation and Conventional Counterforce: The Case of Iraq
- Shibboleth Slaying in a Post-Saddam Iraq
- After Arafat
- Will Saddam Seek to Extend His Presidency?
- Iraq: Next Phase in the Campaign?
- Iraq: The Weapons Inspection Conundrum
- Will the Israeli-Palestinian Conflict Impede the War on Terrorism?
- U.S. Security Architecture in the Gulf: Elements and Challenges
- Current WMD Challenges in the Middle East

South Asia

- Problems in Using Trade to Counter Terrorism: The Case of Pakistan
- A U.S. Strategy for Achieving Stability in Pakistan: Expanding Educational Opportunities
- Assessing Al Qaeda's WMD Capabilities
- The Loya Jirga, Ethnic Rivalry and Future Afghan Stability

In FY01, a new Research Center, the Center for Contemporary Conflict (CCC), was formed. CCC's initial effort was an innovative new program to bring focused regional security education to deploying forces. This effort was augmented in FY02 to allow the CCC program to develop Strategic Insights which provide web-based, concise monthly analyses of regions and issues critical to U.S. national security.

- India and Pakistan at the Precipice: Two Views
- The Role of Foreign Aid in the War on Terrorism
- Rebuilding Afghanistan
- Afghanistan Military Campaign Enters New Phase
- Standoff Between India and Pakistan
- Pakistan: Coming Out of Praetorian Shadows

Russia and Eurasia

- The Limits of Chinese-Russian Strategic Collaboration
- The Role of Foreign Aid in the War on Terrorism
- Enduring Freedom for Central Asia?
- Russia's Military and Operation Enduring Freedom

East Asia

- China and the Iraq Question
- The Limits of Chinese-Russian Strategic Collaboration
- Constituting the Uyghur in U.S.-China Relations: The Geopolitics of Identity Formation in the War on Terrorism
- China's Upcoming Leadership Changes and the PLA
- Beijing and the American War on Terrorism
- The War on Terrorism in Southeast Asia: Searching for Partners, Delimiting Targets

Latin America

- Civil-Military Relations in Venezuela after 11 April: Beyond Repair?
- Financial and Political Crisis in Argentina: Walking a Wobbly Tightrope

Europe

- Kosovo: Time for the Hard Decisions

Homeland Defense

- Surprise and Intelligence Failure
- The Economic Costs of 9/11
- Intelligence and the Department of Homeland Security
- NORTHCOM to Coordinate DoD Role in Homeland Defense
- Homeland Defense: Ramping Up, But What's the Glide Path?

--continued on page 18

STRATEGIC INSIGHTS, *continued from page 17*

War on Terrorism

- Deterrence and Preemption
- Problems in Using Trade to Counter Terrorism: The Case of Pakistan
- Comparing Threats from Saddam and bin Laden
- Surprise and Intelligence Failure
- The Geneva Conventions, POWs, and the War on Terrorism
- Assessing Al Qaeda's WMD Capabilities
- Constituting the Uyghur in U.S.-China Relations: The Geopolitics of Identity Formation in the War on Terrorism
- A U.S. Strategy for Achieving Stability in Pakistan: Expanding Educational Opportunities
- "Illegal Combatants" and the Law of Armed Conflict
- The Economic Costs of 9/11
- The Role of Foreign Aid in the War on Terrorism
- WMD Proliferation and Conventional Counterforce: The Case of Iraq
- Beijing and the American War on Terrorism
- Iraq: Next Phase in the Campaign?
- Enduring Freedom for Central Asia?
- Will the Israeli-Palestinian Conflict Impede the War on Terrorism?
- Current WMD Challenges in the Middle East
- Russia's Military and Operation Enduring Freedom
- The War on Terrorism in Southeast Asia: Searching for Partners, Delimiting Targets

WMD Proliferation and Counterproliferation

- WMD Proliferation and Conventional Counterforce: The Case of Iraq
- Negative Security Assurances and the Nuclear Posture Review

- Iraq: The Weapons Inspection Conundrum
- Current WMD Challenges in the Middle East

Deterrence and Arms Control

- Nuclear Weapons, War with Iraq, and U.S. Security Strategy in the Middle East
- The New Nuclear Pact and the Post Cold-War Arms Agenda
- Negative Security Assurances and the Nuclear Posture Review
- A Quiet Revolution: The New Nuclear Triad

Strategy

- Deterrence and Preemption
- Nuclear Weapons, War with Iraq, and U.S. Security Strategy in the Middle East
- WMD Proliferation and Conventional Counterforce: The Case of Iraq
- Anniversary: The Battle of Midway

The traffic patterns that Strategic Insights website drew in FY02 indicate that these monthly analyses are raising awareness of the Naval Postgraduate School and its mission. Steady military and government traffic to the site indicates that Strategic Insights have served as a new and effective channel through which NPS can perform its traditional role of educating servicemen and officials about current and emerging security challenges. As evidenced by the significant percentage of traffic that comes from the public at large by way of search engines, publication of Strategic Insights has enabled NPS to reach beyond its traditional audience of servicemen and officials, to play a valuable role in helping to educate American citizens about critical national security issues.

INTEGRATED ASYMMETRIC GOAL ORGANIZATION, *continued from page 11*

sequence of steps in blending works as follows:

First, we have an available blender. No mental spaces are connected to the blender and the blender is waiting for first contact. Next we see an input space arriving at the blender. It connects with the blender and causes the blender to extend connectors at the generic space and input two sides that will set up the blender for combination with the right kinds of mental spaces. The next section shows generic space and input space arriving and making connec-

tion with the blender. Now the blender has three mental spaces connected to it. Finally we see the generic space guiding the projection of information from the inputs into the new blend. After completion, the integrated network of these four mental spaces, starting with the blend, the two input spaces and the generic space move off of the blender leaving it ready to resume blending. The integrated network of mental spaces can also move back onto the

--continued on page 47

DEMONSTRATION OF LINKED UNMANNED AERIAL VEHICLE (UAV) OBSERVATIONS AND ATMOSPHERIC MODEL PREDICTION IN CHEM/BIO ATTACK RESPONSE

Professor Kenneth L. Davidson, Department of Meteorology

Associate Professor Isaac Kaminer, Department of Aeronautics and Astronautics

Research Assistant Professor Douglas Miller, Department of Meteorology

National Research Council Research Associate Vladimir Dobrokhodov

Background

Chemical and biological (ChemBio) weapon attacks have posed a response concern for some time and have gained a renewed focus. The toxic cloud has to be measured and its dispersion predicted to successfully respond to attacks by such weapons. This is a report of an atmosphere model formulation, UAV configuration/instrumentation and field measurement effort to demonstrate and validate a method for the synthesis of measurements and predictions to aid in the response to an attack by chemical and biological weapons. The eventual goal of the demonstration/evaluation of integration of technology is to enable operational units to have a near-real time decision aid, integrated into a command and control net, to assist them in responding in a focused way to a ChemBio attack. This decision aid will be based on atmospheric model predictions of the agent transport and dispersion so that *effective* dispersion can be mapped upstream to the source or downstream to the region to be affected.

The multi-factor problem led to a demonstration attempt to sort out real issues and to calibrate expectations. The demonstration effort, addressing issues in ChemBio attack response, was of the transition of emerging as well as operational capabilities into seamless products based on:

- High resolution models for prediction and assimilation of dynamic atmospheric processes;
- On-demand, near-continuous portable UAV sampling;
- Capabilities in current remote (e.g. LIDAR) and in situ (e.g. tactical dropsonde) measurement of atmosphere; and
- Open-ended information systems architecture.

In addition to the atmospheric modeling/UAV sampling value and linkage, the demonstration included in situ measurements for three evaluation/design reasons:

- Value of mesoscale models for plume history and for initialization of conditions.
- Value added to prediction by operational real-time collection of profiles, e.g. by Tactical Dropsondes or LIDAR, by other assets.

Another new initiative supported by CDTEMS in FY02 was an interdisciplinary program to demonstrate the utility of combining meteorological and oceanographic (METOC) prediction capabilities with Unmanned Aerial Vehicle (UAV) sensor measurements and flight control for rapid decision making required when chemical and biological agents are released.

- Value added by atmospheric sampling on UAV.

Results from the demonstration will form the basis for future selection of several different types of models, data collection and model insertion procedures. One collection procedure is plume dimensions using UAV equipped with an appropriate sensor suite to measure the dispersed agent in the atmosphere. The project drew on resources that currently exist and are being (or soon will be) applied separately to operational descriptions of mesoscale circulation and air-land-sea interaction processes. Furthermore, the basic information system design is open-ended, which will allow the incorporation of advances in real-time data collection, distribution and modeling.

Approach

The approach and procedures were selected to culminate with the Intensive Operation Period (IOP) demonstration designed to simulate a "toxic" plume by releasing a smoker on the grounds of Camp Roberts (Fig. 1), fly a UAV for mapping the dispersing plume, and having supporting atmospheric observations for evaluating assumptions and for ingesting into the atmospheric modeling parameter.

Atmospheric Modeling and Measurement: Leading up to the October 2002 demonstration, a full physics mesoscale model was linked with the simple physics model (WOCSS) and post-processing code to create trajectories. The WOCSS model forms the operational basis for the prediction of the origin and destination of the tracer plume given the UAV-mapped plume location and cross-wind structure. A demonstration of the capabilities was completed over a period from 2 October through 5 November 2002, with an IOP from 7 to 11 November 2002. During the 2 October through

--continued on page 20

DEMONSTRATION OF LINKED UNMANNED AERIAL VEHICLE OBSERVATIONS, *continued from page 19*

5 November period, the model was run for a mesoscale region surrounding Camp Roberts, CA and in situ meteorological data collection were made at McMillan Airfield on Camp Roberts. For demonstration purposes, all atmospheric modeling components were self-contained on a SGI multiprocessor UNIX compute server located at the Naval Postgraduate School.

Atmospheric Modeling: Because of the role of the atmosphere in the dispersion, an essential component in the demonstration is the measurement, analysis and prediction of its structure. The use of numerical models to predict weather is widespread. The class of models focusing on small-scale

weather phenomena, known as mesoscale models, is commonly applied to plume dispersion. In a research mode, the mesoscale models have been run at horizontal grid spacing as small as 1 kilometer. In an operational setting, running models at such fine resolutions is impractical, since the computation time required is often greater than the lead-time of the forecast. Also, many of the model physics schemes were developed at a time when grid spacing were much larger and, hence, many of the simplifying approximations used in streamlining the code might not be applicable at fine resolutions.

Central to the methodology is a non-hydrostatic mesoscale model. The role of the mesoscale model is to transform information from large scales in a dynamically consistent fashion down to scales that are resolvable by the finest model grid domain. What is first required for successful implementation



Figure 1. McMillan Airfield, Camp Roberts, California.

of the mesoscale model is the large-scale view of the atmosphere. A large-scale operational model was used as the first-guess with provisions for corrections based on standard observations (e.g. National Weather Service surface and upper-air observations) and "special" observations (e.g. aircraft data, remotely piloted aircraft data). How these various data sources are blended is important because, if they aren't combined in a way that the model "likes," information provided by them will be lost as the model establishes its version of proper dynamic and thermodynamic balance.

The Penn State/National Center for Atmospheric Research (NCAR) Mesoscale Model version 5 (MM5), which has been widely used for research programs sponsored by the Air Force, was incorporated into the demonstration scenario, generating quasi-operational forecasts twice daily at the finest horizontal

--continued on page 21

DEMONSTRATION OF LINKED UNMANNED AERIAL VEHICLE OBSERVATIONS, *continued from page 19*

grid spacing of 9-12 kilometers. However, this model cannot be run on a field compatible laptop. Rather, output from these external location predictions were used to provide 4D data to the demonstrated field compatible trajectory model, Wind Over Constant Streamline Surfaces (WOCSS). Hence, the mesoscale model was linked both operationally and in research mode to a simple physics model (WOCSS) that has terrain elevation information at grid spacing of 100 meters. The overall linkage of models and measurement is shown in Figure 2.

The WOCSS-adjusted wind fields were used to compute trajectories that can characterize the past and future three-dimensional path of the toxic plume. The WOCSS horizontal grid scale is by no means limited to the 1-3 kilometer range in current use at NPS; rather, it is limited by the resolution of available terrain elevation information. A typical mesoscale model 36-h forecast requires 3-h actual wall clock time for completion which, when input to WOCSS requires 30 minutes to adjust the wind fields when model forecasts are output every three hours.

The full physics mesoscale model forecasts were output every 15 minutes over a large forecast volume and are con-

verted into the format required by WOCSS to be defined for a smaller forecast demonstration location volume. One of the tested features was the WOCSS wind adjustment process. As the mesoscale model output frequency increases and the WOCSS horizontal grid scale decreases, the total WOCSS wind adjustment process increases beyond 30 minutes, dependent on the exact specifications of the WOCSS forecast volume. The WOCSS-adjusted three-dimensional wind fields were used as input for a trajectory code capable of deriving backward and forward trajectories from a defined location in space and time. An archive of re-adjusted WOCSS wind fields was maintained as in situ observations were received and used to correct WOCSS fields. The difference between the re-adjusted and original WOCSS wind fields serve as a basis for defining uncertainty in the predicted forward trajectories.

Atmospheric Measurement: The atmospheric measurement and data assimilation approach was to compare time and spatial scales of predicted and actual atmospheric properties that influence dispersion. With such attention to fine-scale atmospheric details, it was necessary to evaluate the suitability of initial prediction and to correct prediction errors that

--continued on page 49

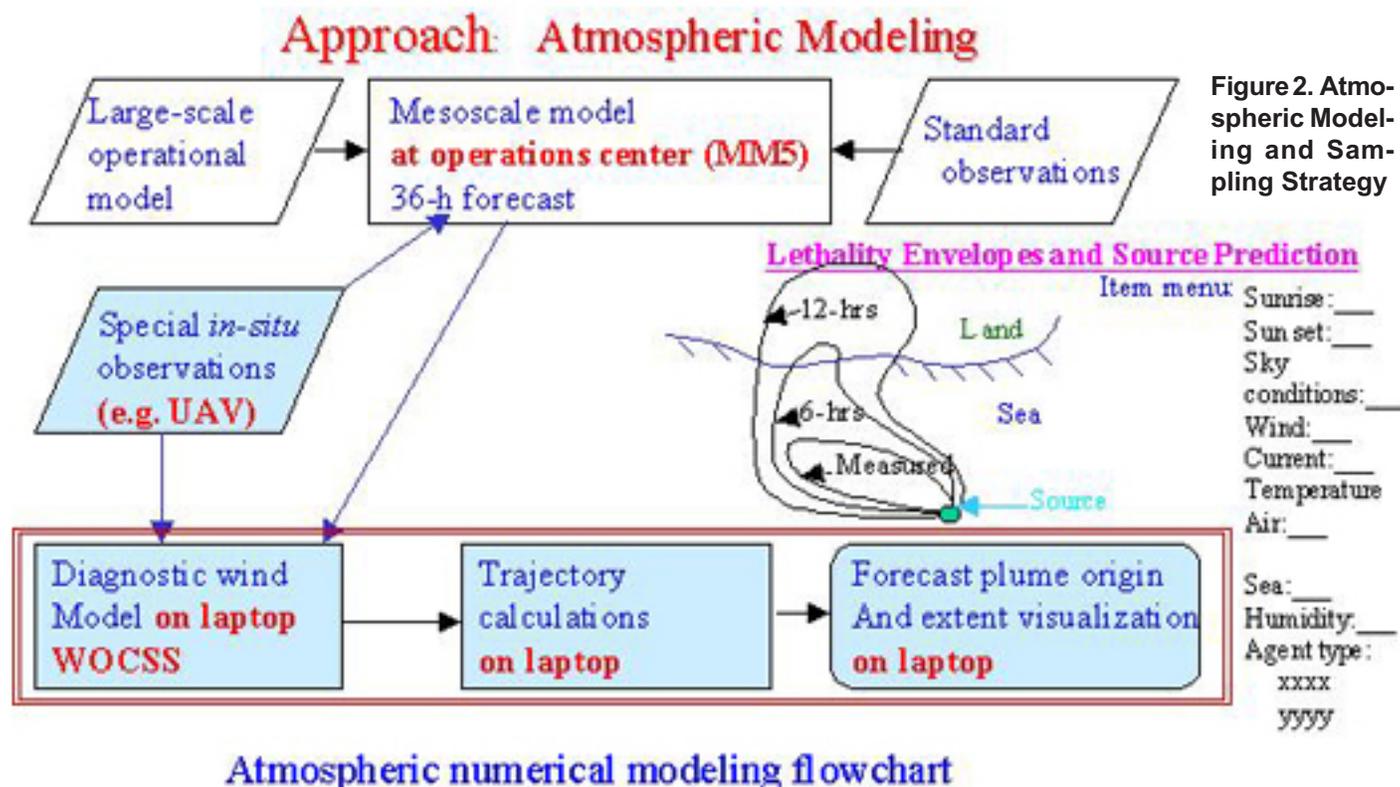


Figure 2. Atmospheric Modeling and Sampling Strategy

FLEET TRANSIT PROGRAM

CDTEMS supports an innovative Fleet-Transit Program in which faculty and students are able to evaluate some of their latest science and technology and demonstrate its value to the Fleet as it transits off the Monterey coastline.

As a part of CDTEMS we have initiated a program in coordination with VADM Bucchi, Commander Third Fleet. It is called the Fleet Transit Program. The idea is to take advantage of the fleet transits along the Monterey coastline. Faculty and students have the opportunity to test/experiment/demonstrate some of their latest S&T in an operational environment and the Fleet has the opportunity to experience/experiment with these technologies with very small investment of time or resources.

In FY02 we provided a 128 kbs over-the-horizon SATCOM antenna system on our Center for Interdisciplinary Remotely Piloted Aircraft Studies (CIRPAS) Twin Otter. This will provide faculty and students the opportunity to put their experimental apparatus on the aircraft, control the experiment from a lab at NPS while the aircraft flies out to interact with the ship offshore, and receive their data real-time. Multiple experiments are possible on each flight. Flight time and experiment integration onto the aircraft are provided to the investigators so that some of the latest laboratory developed technologies can be readily demonstrated in an operational environment. Several faculty and students have already expressed interest for the initial experiments in FY03. We are also coordinating with the Naval Research Laboratory (West) and the Fleet Numerical Meteorology and Oceanography Center for participation in this program. Each project requires considerable coordination with both C3F and the specific ships that will participate in order to match Fleet schedules with technology availability and to insure that ship personnel can effectively utilize and evaluate the new technologies.

LASER BEACON PROTOTYPE

Capt Ed Hospodar, United States Air Force

The objective of this project was to use portable Laser Beacon Prototype (LBP) to demonstrate enhancements to missile defense and other related technology. The U.S. government funded two different LBPs to provide in-scene references to reduce the bias of sensors supporting missile defense activities. Sensor bias is a significant source of target location error. Both LBPs were tested in the field but have unresolved problems. One of the units did not point the laser beam correctly and was transferred to NPS.

CDTEMS provides for a student fellowship program which permits NPS students to bring knowledge and experience with current operational shortfalls that they obtained in their previous operational tours and work on solutions using their thesis research effort.

The goals of this project are to: 1) Make available a fully mission capable LBP at NPS for research, demonstration, and operational use; 2) Demonstrate improved missile defense capability using operational DoD assets; and 3) Provide a Concept of Operations for deployment and employment of Laser Beacons for crisis areas.

During CY02, Capt Hospodar was able to secure matching funds for his CDTEMS project and complete preliminary coordination with operational assets. He discovered that the scope of the problem included a broken laser in addition to problems with pointing the projection optics. He teamed with Aerospace Corporation to determine the cause of the laser problem – a faulty crystal. He purchased and installed new crystals and aligned internal mirrors to bring output power of the laser to specifications.

Capt Hospodar completed the installation of an astronomical dome housing on the Spanagel Hall roof and moved the laser up to the dome to begin work on the pointing system and calibration. Work is in progress to isolate the problems with the pointing system. Early data show that the pointing system may be more affected by random errors than bias errors.

The project was originally scheduled to be completed in 12 months, however, unforeseen problems with the laser and difficulties with the undocumented computer code delayed work on the pointing system. Work to date has identified two risks:

- The pointing system is a medium risk area. Preliminary azimuth and elevation data indicates the possibility that the pointing system has random errors that exceed the pointing specification. These errors are probably caused by corrosion in the bearings and are beyond the scope of this project to correct. An alternative strategy to correcting this problem

--continued on page 23

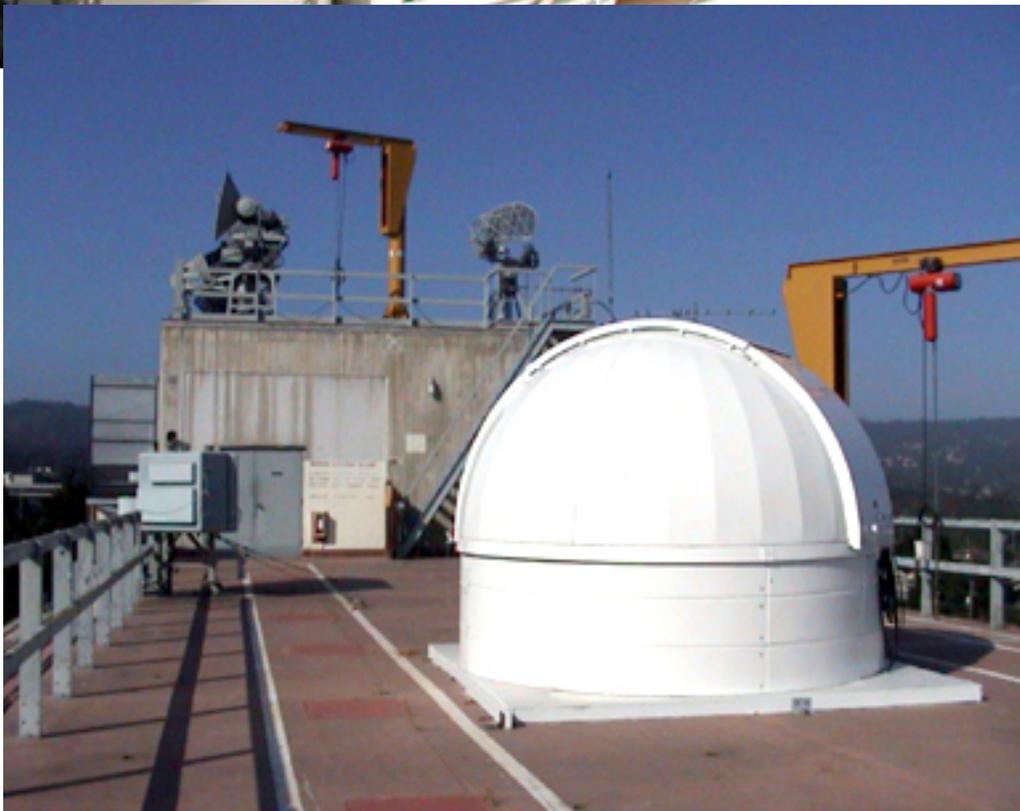
LASER BEACON PROTOTYPE, *continued from page 22*



would be to diverge the beam. This has the negative effect of reducing the output power. If this alternative is implemented, the spec could still be met. Additionally, the undocumented code that controls the system represents a previously unidentified risk to the project. It is unclear at this time whether rewriting the entire code would be more expedient than working with the existing code.

- Planning, coordinating, and executing the demonstrations is a medium risk. Any time operational systems and organizations are involved there is some programmatic and schedule risk. This risk is mitigated by the use of Systems Program Office (SPO) contacts to facilitate operational interaction. The cost of mitigating this risk is included in the request for technical and research assistance and in the travel funds.

More data must be taken to determine the true causes of pointing errors. Additional optics may need to be purchased to diverge the beam if the random errors are the largest source of problems in the pointing system. This represents a significant schedule risk. Also, the control laws, software, and hardware must be evaluated to determine if the tracking system is sufficient (once the instantaneous pointing problems are corrected).



Laser Beacon Prototype (top).

Astronomical Dome Housing on Spanagel Hall Roof (left).

INTEGRATED THEATER ASSESSMENT PROFILING SYSTEM

Capt Michael P. Hadley, United State Marine Corps,

Master of Science in Information Technology Management and Computer Science – September 2002

LT James A. Wiest, United States Navy, Master of Science in Information Technology – September 2002

Introduction

The Integrated Theater Assessment Profiling System (iTAPS) was born of the stove-piped Theater Assessment Profiling System (TAPS) in use by the Second Fleet Staff. The system is a decision support system that is used to synthesize data for the Commander, Second Fleet and his staff to help them assess how operations in progress are performing. Basically, it uses data (grades and comments) input from the Second Fleet staff to create weighted grades in top level functional areas.

The Paradigm

A tree-diagram model with parent and child nodes is an appropriate way to describe iTAPS. Basically, there are areas of the operation that are assigned and graded by personnel on the Second Fleet staff. There can be hundreds, if not thousands of areas to be graded. This fine granularity is synthesized upwards into more general categories by weighting the grades as the Commander desires. The data is ultimately synthesized into a top-level display as seen in Figure 1. This display has categories which synthesize all the data “below” that tier in the system. In this way, an area that requires additional attention can be identified and drilled-down into by the Commander to get finer resolution. This helps the Commander focus his limited resources quickly where his attention is most needed so he or she can make timely, correct decisions in time of conflict.

History

The format of using context-driven radar diagrams had actually been shopped by a contractor to Second Fleet but was too unwieldy and expensive to be of use. CAPT Oliver, the Second Fleet J6 (Command, Control, Communication, Comput-

ers (C4) Systems/Chief Information Officer) wrote an application using currently available Microsoft Office components (Access, Excel and PowerPoint) to duplicate much of the functionality of the contractor product. The problem was that

--continued on page 25

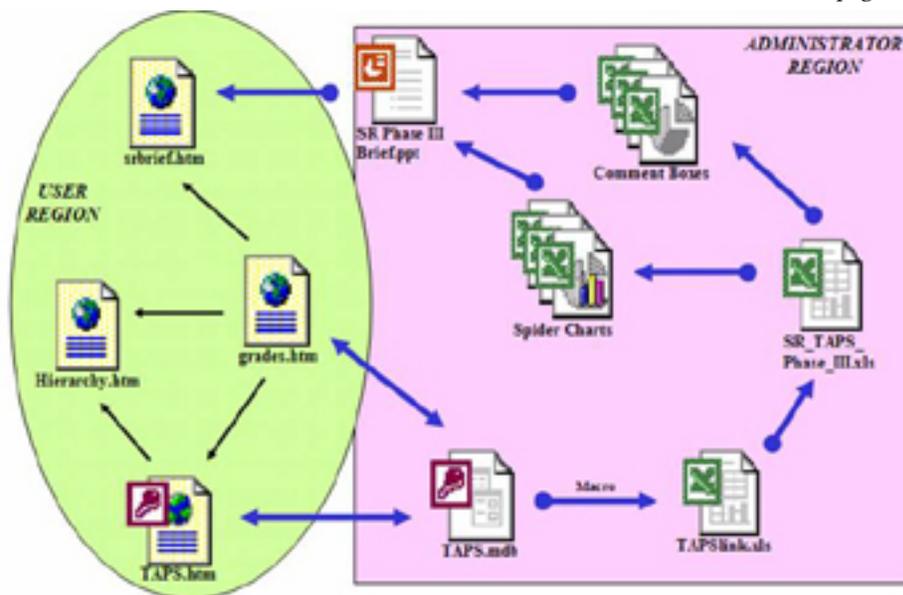


Figure 1. ITAPS top level display.

“Some time ago, as you are already aware, we partnered with Microsoft and NPS to take our home-built Theater Assessment visual tool (TAPS) to the next generation. This resulted in two profound things, (1) we demonstrated the high order benefits of a direct partnership with NPS and private industry, and (2) we have a product that leverages the emerging .net technologies – making our “picture” a product of numerous feeds and sources, regardless of the platform or system. Everyone is a winner in this sort of endeavor: private industry gleans insight into the inner workings and requirements of their biggest customer, the Post Graduate School curriculum connects directly with the evolving fleet issues, and we get something tangible and beneficial that we can put to use right away. I am going to look for other opportunities to partner like this again as we embrace SP21 experimentation.

The two students produced a thesis as their capstone achievement. A summary is posted below, but the full thesis is available at: http://theses.nps.navy.mil/02sep_Hadley_Wiest.pdf.”

....E-mail from VADM Cutler Dawson, USN, Commander, Second Fleet

INTEGRATED THEATER ASSESSMENT PROFILING SYSTEM, *continued from page 24*

this application was also stovepiped, un-networked and non-dynamic. It also required significant man-hours to husband and maintain. CAPT Oliver was an NPS graduate so he took the initiative to contact the NPS Information Systems Program Officer to ask for thesis student support to make the program truly usable across their sizable network.

The Thesis

A student team comprised of a Navy Lieutenant and a Marine Corps Captain, both Information Technology Management students took on the challenge. The goal of the project was simple: Can a web-based, easy-to-use version of TAPS be made that eliminates the stovepiping while preserving all functionality?

Fundamentally the task was one of eliminating the

layers of the current system and utilizing the best web-tools at hand to give Second Fleet something that required minimal maintenance and upkeep. Since Second Fleet is standardized on Microsoft products it was deemed reasonable to utilize Microsoft products for maximum compatibility within the network.

Data Layer

The TAPS MS Access database model was deemed inadequate due to its limited functionality and scalability so a switch to SQL Server was made for the database. This required the thesis students to create a truly relational product that was not a part of the original TAPS. The relational model can be seen in Figure 2.

--continued on page 26

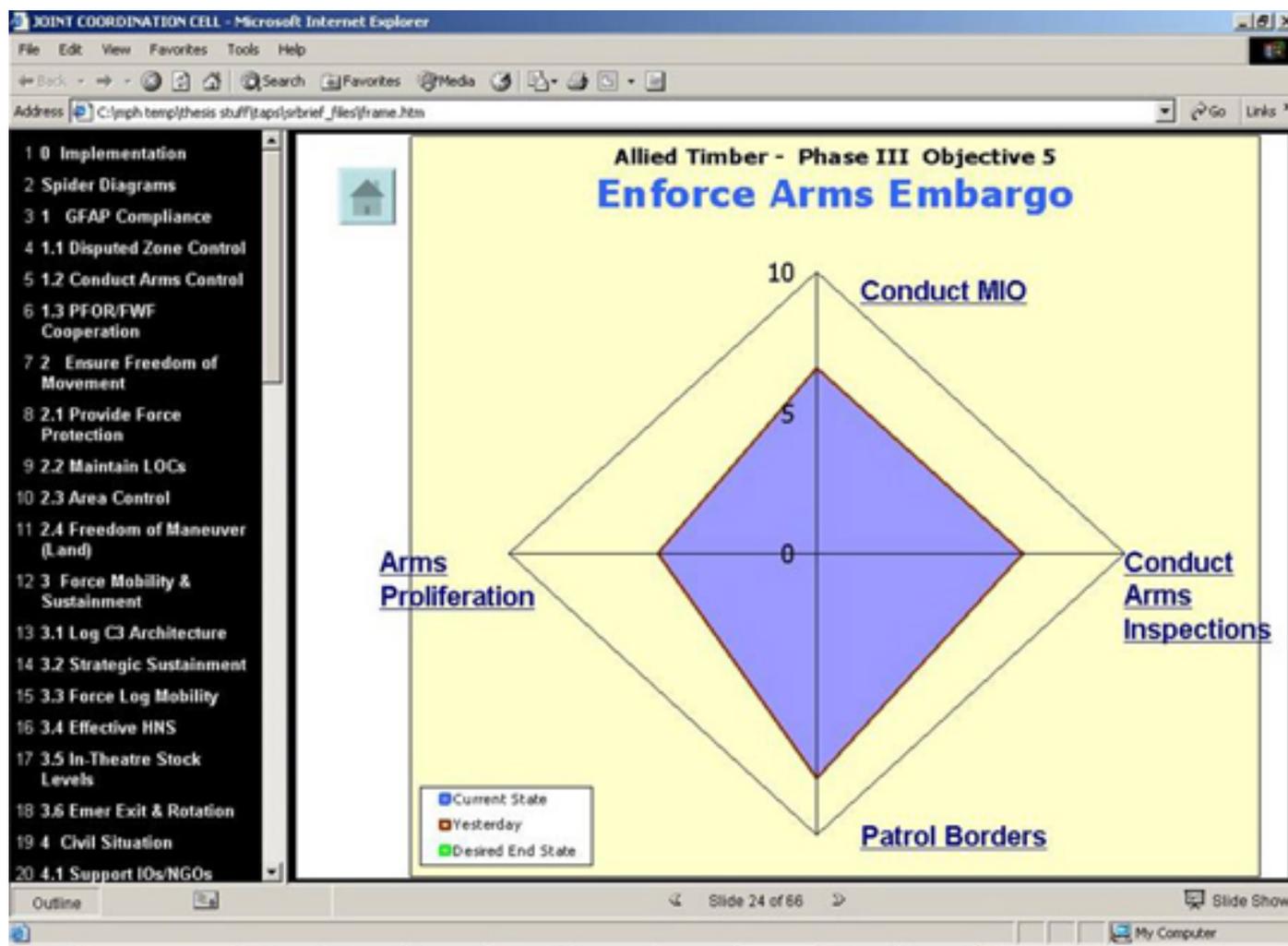


Figure 2. ITAPS Relational Model.

SHIPBOARD INTEGRATED TACTICAL TEAM

LTC Paul Mullin, USA, a recent U.S. Army Fellow in the Department of Defense Analysis, and LT Jon Bartee, USN, a recent graduate of the Combat Systems curriculum, published the front-page article, "Put a SWAT Team on Every Ship: Intercepting Ships in the Gulf," in *USNI Proceedings*, December 2002 issue. The article proposed the tactical concept of a Shipboard Integrated Tactical Team (SITT) and was developed by LT Bartee and LTC Mullin working with an interdisciplinary team of Surface Warfare officers, Army Special Operations officers, Navy SEALs, and NPS faculty.

The SITT concept combines two existing ship-board teams that currently conduct ship's self defense and Visit, Board, Search, and Seizure (VBSS) operations during Maritime Interdiction Operations. LTC Mullin and LT Bartee conducted a mission analysis review of these teams, highlighted capability shortfalls, conducted seminars with subject matter experts, wargamed, then prepared a new concept that included manning, training, and equipping a team to fill the potential dangerous functions of high-seas boardings, inspections, seizures, and ship's self defense.

LT Bartee used CDTEMS resources to develop and present this concept, while participating in a Naval War College Maritime Interdiction war game sponsored by the CNO staff. The Navy is considering the SITT concept for implementation.

INTEGRATED THEATER ASSESSMENT PROFILING SYSTEM, *continued from page 25*

Application Layer

Several products were considered for the application layer, including JAVA and Shockwave as well as others. The main problem with these products is that they require installation and maintenance of the software on hundreds of machines across the network...a significant burden to the Second



**LT James A. Wiest,
USN**

Fleet IT personnel. Avoiding this type of burden was a sub-goal of the project. Fortunately, Microsoft has just released its .Net Framework and it fit the needs of the project exactly. No client-side maintenance or updates beyond a browser (which Second Fleet was already maintaining) was required. Using this foundation, the web-based portals for viewers, administrators and graders took shape. Since SQL Server was used there were seamless links between the data and application layers. Standardizing on a Microsoft solution also enabled integrated authentication using NT user permissions and accounts already in place at Second Fleet, eliminating the need for a separate iTAPS database of users to be created and maintained. The Second Fleet IT department could simply add a user to the group with the appropriate access and SQL Server and the .Net application would validate based on those credentials. This was a significant "work smarter not harder" aspect of going with a Microsoft solution.

The presentation layer was Internet Explorer 5.5+; something that Second Fleet already had in use across its Windows network.

Implementation

Fundamentally, the project was coded by two DoN officers in about three months time using strict criteria established with Second Fleet: 1) No new features required; 2) Minimize software maintenance requirements; and 3) Duplicate existing functionality 100%.

These goals were met. In addition, more features were added by the programmers to make the program more user friendly and expansion ready. The software was installed and made operational in a single day. Second Fleet strongly desires that this software be updated and maintained by subsequent thesis students.

This thesis project is an example of how NPS can directly serve the fleet and demonstrate how relevant NPS is to current fleet needs. It normally takes long lead times and requires significant funds to implement a project like this in DoD and NPS provided this service within an 8-month timeframe with minimal funds. This project was specifically mentioned in a congratulatory letter sent by Commander, Second Fleet to the Superintendent of Naval Postgraduate School.



**Capt Michael P.
Hadley, USMC**

EXPERIMENTAL ANALYSIS OF THE INTEGRATION OF UNMANNED AERIAL VEHICLES AND NAVAL SPECIAL WARFARE OPERATIONS

LT Joseph Clayton Butner IV, United States Navy
Master of Science in Defense Analysis – December 2002

A broad military use of Unmanned Aerial Vehicles (UAVs) has emerged over time with the evolving increase in UAV capabilities (*UAV Roadmap 2025*, 2001). The usefulness of UAVs is evident by their successful use in the War on Terror in Afghanistan, or as seen by the recent Predator missile attack in Yemen on an al-Qaeda terrorist, Ali Aqed Sinan al-Harthi, also known as Abu Ali, (*USA Today*, 05 Nov 02). However, these high profile missions also demonstrate a limitation. Predator, Global Hawk, and other UAVs like them are limited in number and expensive, and therefore are considered strategic assets. In fact, according to the Joint Special Operations Air Component Commander (JSOACC) during operation Enduring Freedom in Afghanistan, Col J. Tyner, USAF, it was easier for special operations forces to get support from B52s to drop bombs than it was for those same forces to get UAV support to “see what was over the next hill” (Tyner, 2002). A study of how Special Operations Forces (SOF) should best use UAVs determined:

Control of SOF UAVs should go to those best able to utilize them with the general goal to push them as far down in the chain of command as makes sense. In other words, commanders should seek to empower small units without unnecessarily burdening them. (James, p. xiv)

We wanted to investigate whether or not small, inexpensive/expendable, long endurance, UAVs may significantly increase the combat effectiveness of Navy Special Warfare (NSW) forces. They should be small to be stealthy, transportable, easy to launch, and low cost. They need to be long endurance so that they can be launched before SOF insertion and remain on site until after mission completion, with minimal or no aircraft/payload control required of the forward forces. They need to be low cost for obvious reasons, but primarily so that they can be launched and left; eliminating the need for recovery and the logistics required for reusable assets. To accomplish this objective a small field experiment was planned and executed in which modeling and simulation was used to help select the test environment and variables, to determine the most desirable UAV flight patterns, and to develop quantitative measures of effectiveness (MOEs).

Based upon the investigator’s personal knowledge and experience with current SOF missions and operating pro-

In FY02, CDTEMS supported a limited objective field experiment to demonstrate the utility for utilizing multiple, expendable, small Unmanned Aerial Vehicles (UAVs) with Navy Special Warfare Forces (NSW) for enhancement of the downed-pilot-rescue mission.

cedures, it was decided to focus this initial experiment on downed-pilot rescue; a mission for which the UAVs have potential for significantly improving concepts of operations. To develop interest and participation and to obtain recommendations for conducting the LOE a number of facilities and commands were visited; Commander Third Fleet, Naval Special Warfare Command, Naval Special Warfare Development Group, Naval Special Warfare Group 2, Office of Force Transformation, Office of Naval Research, Center for Naval Analysis, Naval Surface Warfare Center Carderock Division, the Lawrence Livermore National Laboratory (LLNL), and the Schafer Corporation in coordination with DARPA.

In order to complete this investigation, the cooperation and help of many people and organizations both within NPS and external was required. The NPS Center for Defense Technology and Education for the Military Services (CDTEMS) provided financial support and coordination. The Director of the NPS Wayne E. Meyer Institute of Systems Engineering provided assistance with the experimentation, plans for data collection and analysis, etc. Students in the Models of Conflict course (SO4410) developed models for the experiment variables and MOEs. This helped determine the feasibility of the experiment by analyzing the force (red and blue) distributions within the search areas and the probability of the forces detecting each other. An example of the results is shown in Figure 1.

Students in the Systems Engineering and Integration curriculum Naval Tactical Analysis class (OS3680) developed models which provided the optimum flight patterns for both the pilot-search and command-and-control (C2) UAVs. These models were based upon the requirements for having a one-km diameter of situational awareness. This one kilometer diameter is an estimate of the distance required for a SEAL patrol to react to the ability of an enemy force to detect a moving SEAL patrol (or pilot) without sensors in a variety of terrain (and have enough warning to evade detection). The

--continued on page 28

INTEGRATION OF UNMANNED AERIAL VEHICLES AND NAVAL SPECIAL WARFARE OPERATIONS, *continued from page 27*

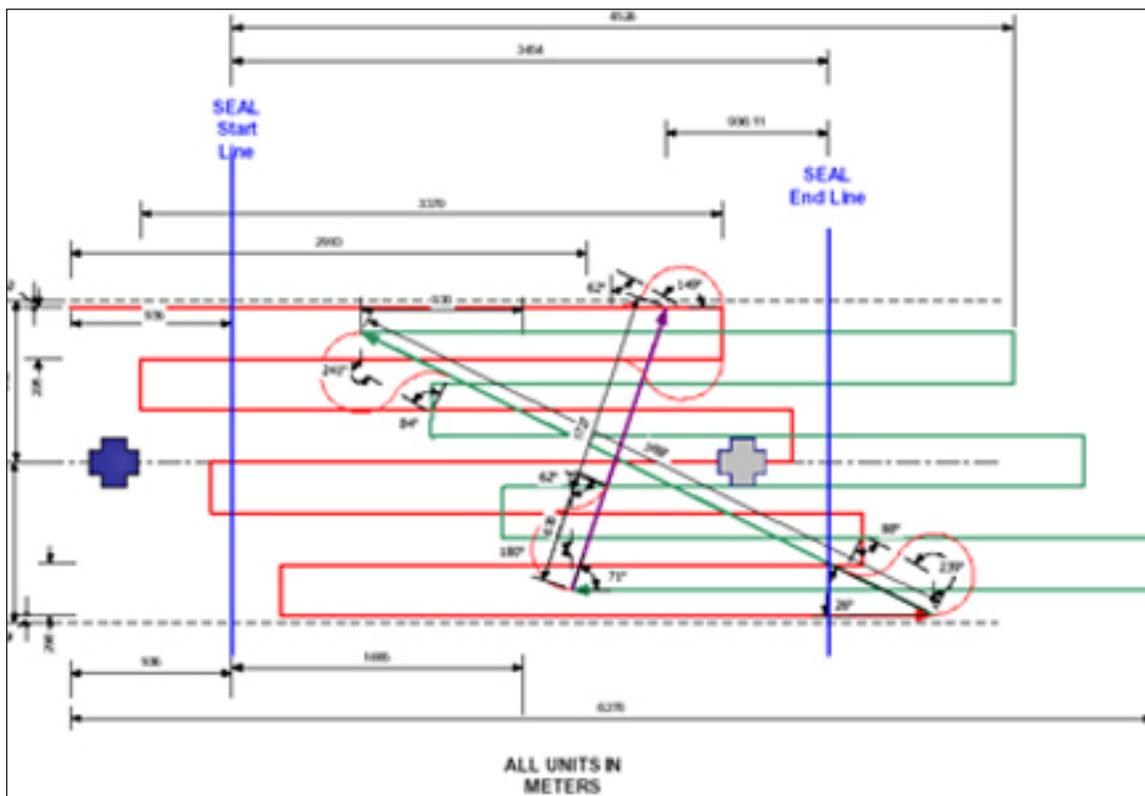
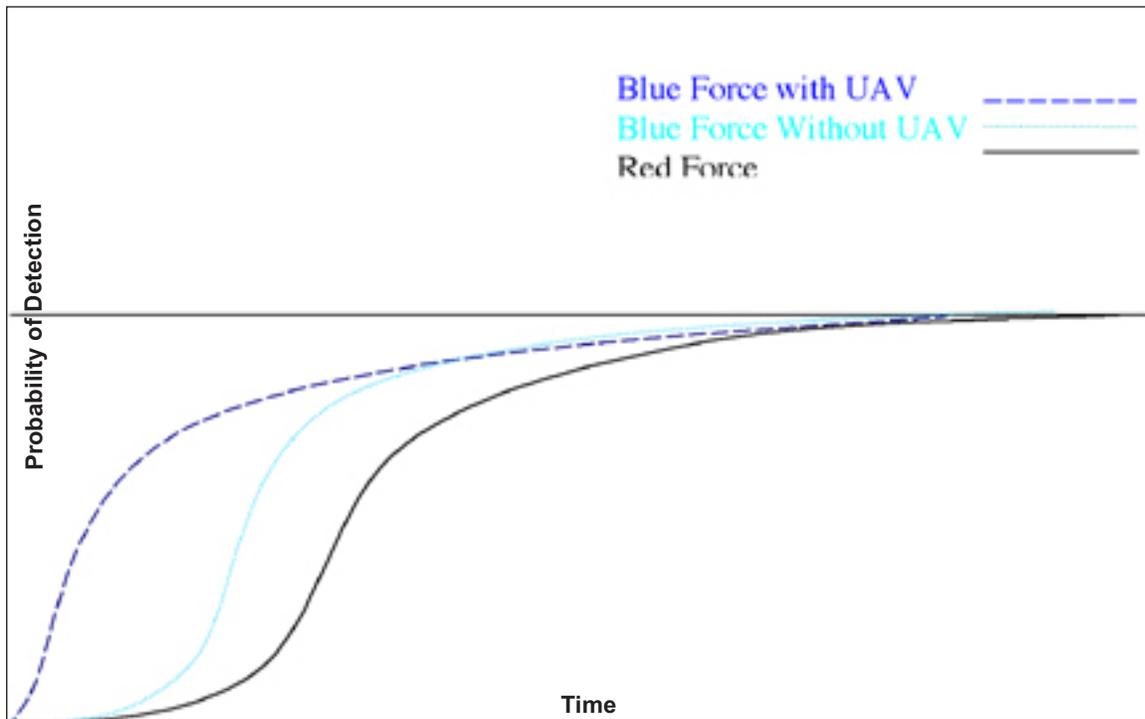
models also had to take into account the speed and turning radius of the UAV and the field of view of the low-light camera. An example of the results for the C2 UAV is shown in Figure 2.

Cpt Alistair Dickie (Australian Army) had previously conducted thesis research and developed an agent-based simulation to demonstrate the possible swarming characteristics of UAVs, called MARSS (Multi-Agent Robotic Swarm Simulation). He modified his model to examine a simplified version of our experiment. It showed that the intelligence provided to the red team had to be increased (smaller search area) if the base experiment without UAVs was not

--continued on page 29

Figure 1 (above right). Cumulative probability of detection taking into account available intelligence information

Figure 2 (right). Patrol/C2 UAV Flight Pattern.



INTEGRATION OF UNMANNED AERIAL VEHICLES AND NAVAL SPECIAL WARFARE OPERATIONS, *continued from page 28*

to result in the blue team having a nearly 100% success rate in locating the downed-pilot before the red team. The experiment plan was modified accordingly.

The UAVs were provided by Advanced Ceramics Research (ACR), Tucson, AZ. The SWARM vehicle was initially desired for utilization but at its current state of development it did not have the desired endurance, level of night vision, nor the image resolution at flight speed. Thus, a commercially available UAV (standard high wing trainer) was utilized using ACR avionics and controls. It had an approximately two-hour endurance and a low-light (0.0003 LUX CCD) camera as payload. Figure 3 shows the SWARM being catapult launched at the NPS Center for Interdisciplinary Remotely Piloted Aircraft Studies (CIRPAS) UAV test facility, Camp Roberts, CA. Also shown on the ground is the Standard Trainer UAV. IR strobes were placed on all forces to permit the available camera to detect them while flying as high as 4000' AGL.

Airfield coordination and use was provided by CIRPAS. The Blue Force and C2 element members were provided by seven Navy SEALs from the Naval Coastal Systems Station, Panama City, FL and the Defense Language Institute (DLI), Monterey, CA. Ten enlisted Navy students at DLI provided the Red Team and downed-pilot.

While SEAL patrols normally consist of a minimum of eight personnel, depending on the mission, two were considered to be adequate for purposes of this experiment. The additional SEALs in a patrol provide extra fire power and mission essential skills, but the standard operating procedures (SOPs) for two SEALs on patrol are basically the same as for eight. The footprint, or signature of their presence is reduced, but this should have minimal effects on the data to be analyzed. Additionally, a limited number of red force and blue force personnel were available. The use of two blue force personnel per search element meant that the red force element, made up of four personnel, would be double the size of the blue force. A red force double the size of the blue force was used in all modeling and simulation.

The experiment was designed to consist of a total of ten Combat Search and Rescue (CSAR) missions conducted at Camp Roberts, CA. There were two SEAL search teams, each with two personnel. The remaining SEALs were part of the Command and Control (C2) element, one C2 element with one SEAL and one C2 element with two SEALs. A two by four-kilometer op area was chosen to allow for the maximum amount of data points to be collected while still being able to conduct the mission within a single cycle of darkness. Five

--continued on page 30

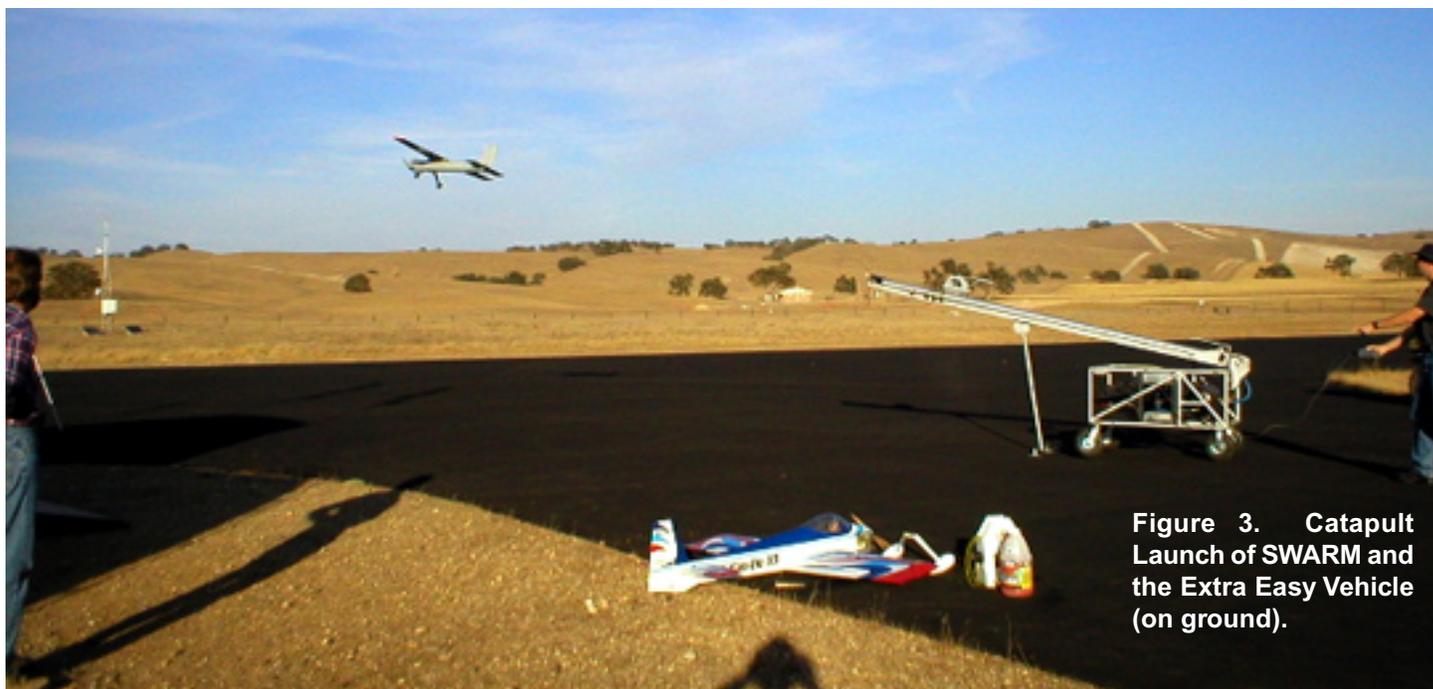


Figure 3. Catapult Launch of SWARM and the Extra Easy Vehicle (on ground).

INTEGRATION OF UNMANNED AERIAL VEHICLES AND NAVAL SPECIAL WARFARE OPERATIONS, *continued from page 29*

of these op areas were then chosen for their varying terrain and to ensure that participants were not operating in familiar territory. Personnel locations were to be changed in each op area to prevent any bias from a previous night's mission. Each op area was to host two separate teams conducting the same mission on different nights. However, one team would be assisted by two tactical UAVs and one team would not. The op areas were to be used in a random order and the NSW search teams would not know what op area they would be inserted into until the night of the operation, nor would they know if they were to be assisted by UAVs until that night. This was to ensure teams could not help one another plan for that night's mission. The scenario within one particular op area was exactly the same for each team except for the UAVs. All participants in a given op area were inserted in the exact same location as the other group that had utilized that op area the night before. The insertion locations of the participants relative to each other varied with each op area. Nightly missions were to continue for a total of five nights, until both teams conducted all the same scenarios one time. This, however, was not accomplished, and only two separate nights of missions were conducted (discussed below). Each mission scenario varied only by location of crash sight, pilot, red cell, NSW team insertion point, and the geographical and terrain differences among the op areas. Distances between forces were nearly identical. This would allow for direct comparison of missions conducted in the same op area and a general

comparison of missions conducted in other op areas.

Experiment observers were to track actual movements conducted by all participants to verify actual C2 and ground force situational awareness. A number of different recording methods were available to help track movements and gather data, such as UAV over-flight recording tactical UAV movement, voice recording, manual note taking, and GPS way-point tracking. For each experiment the number of Blue Force detections of Red Forces, the time-to-link between Blue Forces and pilot, whether or not there was a positive link made, and the number of detections by Red Force of Blue Force or pilot were recorded. Questionnaires were also utilized to obtain qualitative data from all participants after each experiment.

While most of the initially selected operational areas were utilized, the UAVs were unable to fly outside of visual range from the McMillan Assault Strip at Camp Roberts due to liability insurance issues for autonomous flight which were thought to have been resolved (a lesson learned regarding detailed planning requirements). This, of course, negatively impacted the design of the experiment. In addition, severe weather resulted in cancellation of the last two nights of operation. In addition, limited-line-of sight flights were conducted to test equipment and the user interface, and secondary autonomous flights were conducted during 4-6 December 02 in a new location (Tucson, AZ). While a direct correlation between the missions with the UAV and those without could

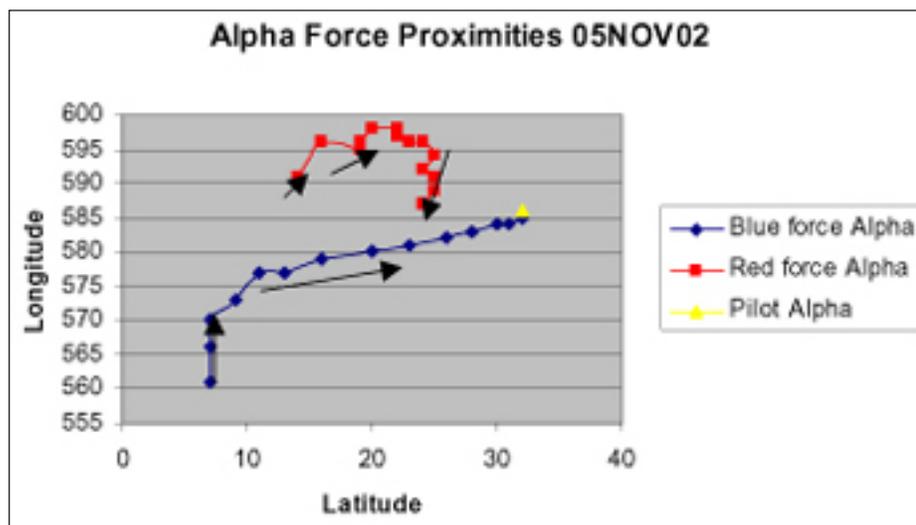


Figure 4. Red and Blue Force Tracks without UAVs Conducting Downed-Pilot Rescue.

no longer be made, enough data was gathered to make strong inferences of effects on the identified MOEs.

The primary MOE utilized was situational awareness. Figure 4 shows one example of the paths taken by red and blue forces and the pilot without UAVs in a night experiment. Each mark represents the actual GPS location which was taken every ten minutes by the ground forces. These locations were to have been compared to a second group of forces utilizing a UAV. The closest proximity of red forces and blue forces or blue forces and the downed pilot could then be compared for missions with and without the use of UAVs. Situational awareness was measured

--continued on page 31

INTEGRATION OF UNMANNED AERIAL VEHICLES AND NAVAL SPECIAL WARFARE OPERATIONS, *continued from page 29*

by the difference between a force's actual (GPS) location and the C2 element's estimate of their location. Due to the fact that the UAVs were unable to fly the profiles originally anticipated, the quantitative data that could have been directly compared to the data without UAVs was unobtainable. Instead, data collected from separate flights, without ground forces, and with IR strobes representing fixed force locations had to be interpreted. These outside-scenario flights were treated as a snapshot of the events that occurred during the original scenario that had moving troops on the ground. This allowed the data taken with the UAV to be compared to a single set of data taken from the experiment with ground forces but without UAVs.

Table 1 shows the Blue Force situational awareness (SA) data for the experiment shown in Figure 4. The two columns beneath "GPS track" contain the actual GPS location of the Blue force in six digit grid coordinates. For example, Wave Point (WP) 1 UTM grid location is 007561, WP 3 UTM grid location is 007566. There are many data points for a single force as the force was on the move, and the points started at the beginning of the mission and ended when the pilot was located. The red force and downed pilot positions were recorded in separate tables. The next two columns under "C2 estimate" contain the C2 element's best guess as to where the blue force was located. When the location matched exactly, this usually indicated a point when the blue force

called back to the C2 element with a position update, which occurred only once an hour. The "difference" columns present the difference in hundreds of meters between the actual force location and the C2 element's estimate. The absolute value represents the SA difference between the actual force location and the C2's estimate. The SA differences are added at the bottom of the table and the average value is also given. The lower the number or difference the better. An SA difference of zero would indicate that the C2 element knew exactly where the blue force was located. The higher the number, the greater the error in estimation or the poorer the SA.

Four sorties of UAV flights that lasted just under one hour each were flown over the Tucson op area to locate the three separate forces (IR strobes). The C2 element (one Army SF MAJ) observed the video screen in the tactical operation center (TOC) next to the UAV pilot. When the C2 element observed a strobe, the UAV pilot was informed, and the UAV pilot provided a verbal location of the UAV in latitude and longitude (later converted to Universal Transverse Mercator (UTM) grid

--continued on page 52

Mission # 2 (05NOV02), Alpha Forces								
WP	Blue Force GPS Track		C2 Estimate		Difference E	Difference N	Absolute Value Situational Awareness Difference	
	E	N	E	N				
1	7	561	8	560	-1	1	2	
2	7	561	6	565	1	-4	5	
3	7	566	7	570	0	-4	4	
4	7	570	11	573	-4	-3	7	
5	9	573	14	578	-5	-5	10	
6	11	577	12	575	-1	2	3	
7	13	577	19	576	-6	1	7	
8	13	577	23	579	-10	-2	12	
9	16	579	27	580	-11	-1	12	
10	20	580	31	583	-11	-3	14	
11	20	580	33	584	-13	-4	17	
12	20	580	24	579	-4	1	5	
13	23	581	27	580	-4	1	5	
14	26	582	31	583	-5	-1	6	
15	28	583	32	582	-4	1	5	
16	30	584	33	584	-3	0	3	
17	31	584	33	584	-2	0	2	
18	32	585	33	584	-1	1	2	
Cumulative SA difference								121
Average SA difference								6.7

Table 1. Situational Awareness Data

HOMELAND DEFENSE AND SECURITY: THE NAVAL POSTGRADUATE SCHOOL'S INITIATIVE

The Naval Postgraduate School has long supported the interests of the Department of Defense (DoD) and Department of Navy (DoN) by aligning upper division course content and faculty and student research. Since the events of 11 September 2001, NPS has begun a new initiative to strengthen NPS' ability to help meet a critical national security challenge. In response to the Secretary of Defense's designation of Homeland Security (HLS) as a top priority DoD mission, NPS is leveraging its unique capabilities to accomplish specialized graduate education and research requirements.

Building on existing NPS academic expertise in the areas of critical infrastructure protection (including information systems and networks), counter terrorism, civil military relations, operations research, command, control and communications, modeling and simulation, intelligence, and much more, NPS will utilize its diverse enrollment to strengthen civil military and interagency teamwork. The NPS homeland security initiative will be guided by the creation of a new discipline, research, and the development of a digital library.

The Center for Homeland Security was formed in 2001 under the direction of Associate Professor Paul Stockton, Department of National Security Affairs, and Professor Ted Lewis, Department of Computer Science. The Center is the focal point for coordination of the NPS homeland security initiative and in doing so has obtained support from the Department of Justice (DoJ).

The curriculum and research priorities detailed in an interagency agreement with DoJ focus on opportunities to strengthen the U.S. capacity to deter, defeat and respond to threats to homeland security. Efforts will deal with civil-military and interagency challenges of HLS planning and operations. The curriculum will include both technical and non-technical curriculum components, i.e., protection of critical infrastructure, history, policy, etc. Modeling and simulation will be built into the heart of the curriculum.

The NPS Homeland Security Program is structured for maximum effectiveness and efficiency. The key components are:

- Mobile Education Team Seminars: The goal of this

program is to bring executive level education on HLS to Governors' staff. A typical seminar will last two days and be delivered to major regions of the United States. NPS expects to execute 8-10 seminars per year.

- Executive Education for State Executives: These one-to-two week courses are aimed at senior executives and policymakers. The goal is to provide brief, but intensive, education programs for existing senior leadership in HLS. An additional goal is to build teamwork by enrolling a broad range of participants and regional perspectives (multiple State and Federal agencies). This allows for comparative analysis of different approaches to HLS, strengthens cooperation across disparate Federal agencies, and enhances local/State/Federal understanding and cooperation.
- Masters Degree Curriculum: A Master of Arts in Security Studies with a specialization in HLS has been developed. It is the first Mas-

ters program in the U.S. with a focus on HLS. NPS has developed a hybrid approach for delivery for the 18-month program intended for experienced, high-level public safety administrators. Students will complete two courses per quarter via distributed learning. These courses will consist of online scenario based exercises and research work supported by the HLS e-library at NPS. Students will also spend two weeks in residence at NPS each quarter, one each at the beginning and end of each quarter. The resident modules will serve to launch the two-courses at the beginning of the quarter and allow students to complete and present their research findings at the conclusion of the quarter. Additionally, the NPS Masters program thesis requirement allows for a two-way payback to students sponsors by providing high-quality, low-cost research on topics of concern to sponsors and creating subject matter experts who can help lead future policy development and operational planning efforts.

- Digital Library: The HLS e-library at NPS will support students during their program as well as after graduation. It will be an on-line resource for DoJ, the

--continued on page 33

HOMELAND SECURITY

HOMELAND SECURITY DIGITAL LIBRARY PROJECT

Dr. Maxine Reneker, Principal Investigator
Lillian Gassie, Senior Systems Librarian
Greta Marlatt, Head, Information Services
Lori Emadi, Technical Information Specialist
Layne Williams, Administrative Librarian

The Dudley Knox Library is developing a digital library to support the research and curricula funded by the Department of Justice grant for Homeland Security and Homeland Defense. When completed, this digital repository will provide 24/7 access to relevant information to researchers, scholars, practitioners and decision-makers dealing with homeland security. It will contain web-enabled documents, articles, government publications, state and municipal planning documents, gray literature, multimedia materials and contact information of subject matter experts in the various related fields. It will also provide tools and services to facilitate effective research and collaboration in the area of homeland security.



Dudley Knox Library
Naval Postgraduate School

The Library staff identified the need for the development of this tool as a means of “preserving the current debate” over the issues involved in homeland security. Since no academic discipline exists to examine these issues or prepare personnel for homeland defense, the Library

will contain a very broad range of materials, both in subject and format. For example, project staff will be identifying and adding research studies, news features, white papers and case studies, bibliographies, tools [e.g. simulations, software], congressional materials, and state and local plans. Formats may be multimedia, as well as digitized print.

The development of the Homeland Security Digital Library is being undertaken in three phases. The first phase was developed as a proof of concept,

containing a browse-able list of resources, a search engine, a web interface for submission of new resources, and selected news feeds. The Library staff also undertook preliminary development of a taxonomy for the organization of the digital materials. This development included defining the scope of the taxonomy, examining the standards to be used in creating the records describing the content, the record format, and the metadata fields to describe the content. This alpha phase was completed in October, 2002.

Additional funding was received in the fall, which enabled us to begin the development of Phase 2. This phase of the project includes a refinement of the taxonomy, a more robust website with a customizable user interface, an alerting service, user authentication to enable different levels of access to restricted data, and a knowledge discovery tool. Phase 2 is expected to take approximately 15 months to complete.

Phase 3, if funding continues, will result in an authoritative thesaurus on homeland security, and a collection of comprehensive digital information supported with a real-time virtual reference service, online collaboration among professionals, text mining and data visualization tools.

HOMELAND DEFENSE AND SECURITY,

continued from page 32

Office of Homeland Security, and other local, State and Federal agencies.

- Research and Development: NPS openly solicited proposals from the NPS faculty. In 2002, 28 proposals were considered by an NPS committee appointed by the Dean of Research. Six projects were recommended and approved by the Award Committee and DoJ. A second solicitation has just concluded and additional topics are being recommended to DoJ. Research supported in 2002 focused on: 1) Emergency Response for Cyber Infrastructure Management; 2) Infrared Face Recognition System, 3) Optimizing Electric Grid Design Under Assymmetric Threat, 4) Vulnerability of Wireless Networks, 5) Concealed Weapons Detection, and 6) Intelligent Software Decoys.

HOMELAND SECURITY

ATTACKING AND DEFENDING COMMUNICATIONS NETWORKS

Professor George Dinolt, Department of Computer Science

Research Assistant Professor Kelly Cormican, Department of Operations Research

Introduction

Defense of our nation's cyber-infrastructure is one of the important concerns in homeland security today. This concern is repeatedly expressed in newspaper headlines and technical articles, and is the focus of an entire division in the Department of Homeland Security. In a May 2002 article in the *Wall Street Journal*, former Director of Central Intelligence James Woolsey implores the nation's leadership and all Americans to "take charge of assessing and correcting the vulnerabilities in all of our national networks." Certainly, both motivation and application abound for research on the vulnerabilities of our nation's critical networks. It is in this setting that we set about applying proven operations research techniques for attack and defense of networks to the more specific arena of communications networks. Our approach uses mathematical-programming techniques to determine the optimal locations for network attack over a range of attacker resources, and then uses these results to suggest the best locations to defend (harden) against such attacks. We then confirm the prescribed solutions with simulation.

Background

Over the course of many years, researchers at the Naval Postgraduate School and elsewhere have developed many useful mathematical techniques for the optimal interdiction of different types of networks. The networks include general road, transshipment and flow networks, and applications include combating drug trafficking, destroying wartime supply lines, and inhibiting networks used by terrorists. However, there has been little application to communications networks, where an interdiction can be directly interpreted as an attack on such a network. Therefore, we focus the application of mathematical programming-based network-interdiction techniques to packet-switched networks that do not possess a centralized routing design. For relevance, we consider an example network similar to the evolving Navy-Marine Corps Intranet (NMCI), although the techniques are general enough to be used on other communications networks. We derive a reasonably accurate model of communications-network behavior, attack that model optimally, and then use these results to determine where defenses should be placed. The accuracy of the results is verified through means of simulation.

Model

The model for communications network behavior and attack is derived from models that have proven useful for optimal network-capacity expansion: They determine the locations at which new equipment (switches, cable, etc.) should be placed to best satisfy future demand, subject to budget limitations or other restrictions on that new equipment. In these models, data is taken on network loading over a range of conditions: time of day, day of week, peak loading periods, etc. Using this information, and forecasts of increased loading, it is possible to find the optimal locations to expand the network for the purpose of, for example, minimizing the amount of unserved demand for communications traffic. The most rigorous of these models uses stochastic programming with sampling due to the large size of the resultant problem (e.g., "Network Planning with Random Demand," Sen et. al., *Telecommunications Systems* 3, 1994).

But our situation is the opposite: We find the "optimal" locations to eliminate capacity. Our capacity-eliminating attacks may be interpreted as a physical-layer attacks that result in a shutdown of that portion of the network. (In common network terminology, *physical layer* is a reference to the actual physical components that carry each bit of information in the network. Physical-layer attacks may be contrasted with, for example, routing-layer attacks that could result in packets being delivered to erroneous destinations.) An attack may come from any of several means, such as a bomb at a switching center, a backhoe cutting a fiber link, or even a cyber-attack that results in a shutdown.

Sophisticated or organized attackers may be able to achieve coordinated, near-simultaneous attacks at several locations in the network. In a worst-case scenario for one, two, three, or more coordinated attacks, we use our model to determine the locations having greatest effect: Which network components, no longer available, most significantly decrease the overall capability of the network to transport communications traffic? From the network user's point of view, these components are those that are leading candidates for hardening, where we assume that hardening a component prevents it from being successfully attacked. In fact, it is possible to use an extension to our model to determine the optimal components for hardening subject to a limited "defense budget." In doing so, we answer this ques-

--continued on page 35

ATTACKING AND DEFENDING COMMUNICATIONS NETWORKS, *continued from page 34*

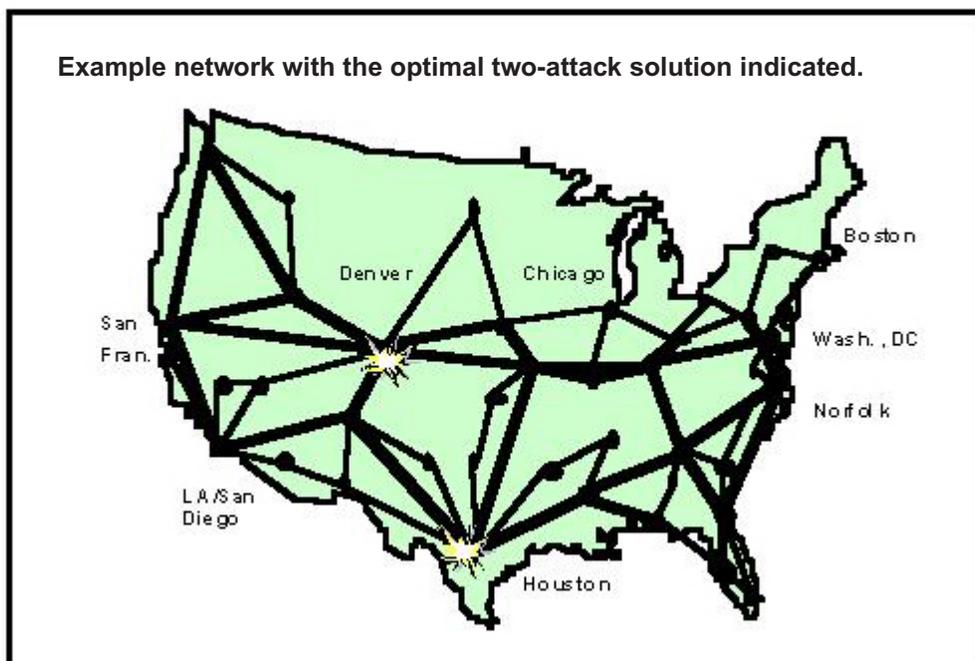
tion: Which network components, if hardened to prevent attack, most significantly decrease the effect of a worst-case attack? In other words, we are interdicting the attacker to prevent the worst-case attacks.

Our approach avoids one of the more vexing questions when dealing with terrorist-style attacks, that of objective. It is difficult to plan against an enemy if you do not know his goals. For example, we make no assumptions that the attacker is attempting to achieve maximum psychological effect, or is attempting to shutdown a particular portion of the network. Rather, we use a measure of effectiveness appropriate for the user of the network (amount of overall communication flow, possibly prioritized by importance) and assume our enemy is capable of initiating a worst-case attack as it applies to overall communication flow. This approach inherently also credits the attacker with the ability to recognize hardening of the network, too. That is, the attacker wastes no resources in a futile attack against a hardened network component. Finally, there are no “time periods” for alternating attack and defense in our model that would suggest a game-theoretic approach. Both network attacker and defender operate with complete knowledge of the state of the network. We believe the resulting model is a conservative one for the network user, just as it should be.

Case Study

Our example network has 43 nodes, which represent routers, switches, or points of origin and/or destination for communications traffic. Connectivity between nodes is achieved with 71 links with bandwidths ranging from 52Mbps to 2.4Gbps. Network traffic is modeled as requests for bandwidth between 50 node pairs. Three scenarios, or “snapshots,” of network loading are constructed, with a 50% probability assigned to the scenario with the highest overall traffic density, and 25% each to the other two. Using a few high-interest scenarios avoids the computational complications of stochastic programming as “previously discussed; whether there is a substantial loss in model fidelity can later be checked via simulation. Feasible traffic routing is determined by generating up to ten

Example network with the optimal two-attack solution indicated.



“near-shortest” paths between node pairs, where the measure of “length” incorporates link bandwidth, node capacity, and propagation delay. (Congestion is not directly considered in this model, although work on a model that will be underway.)

Once several feasible paths are found for each communicating node pair, the model attempts to minimize that maximum communication flow between all the node pairs as previously discussed. This is a bilevel programming problem, which we convert to a more standard mathematical program, a “mixed-integer program.” We repeatedly find a solution to this model while increasing the number of network components that can be attacked, and results are then reviewed. We find that the network is split into two independent pieces after only two (worst-case) attacks, effectively stopping all communications between the east and west coasts in our example network and dropping the overall network flow by half. After eight such attacks, the communications capability of our network is negligible.

In the next step, we harden the two sites that were attacked to split the network, making them invulnerable. The above attack process is repeated, and we find that we preserve up to 15% of the overall demand for communications. For this worst-case attack, we can now more objectively compare the cost of hardening these two network components to the cost of losing 15% of necessary communications.

--continued on page 36

FACE RECOGNITION SYSTEM USING UNCOOLED INFRARED IMAGING

LT Diogo C. Pereira, First Lieutenant, Brazilian Air Force

Associate Professor Monique P. Fargues, Department of Electrical and Computer Engineering

Associate Professor Gamani Karunasiri, Department of Physics

This study investigated the design and implementation of an infrared face recognition system using an uncooled infrared camera. Infrared imaging devices offer several advantages over visible imaging devices, the main one being they are robust to ambient illumination changes, as illustrated in Figure 1 which shows a thermal image taken under room light and complete darkness conditions. To date, the identification of humans using infrared (IR) is carried out using high temperature resolution IR cameras, which are very expensive due to the required cryogenic cooling, making their use prohibitive on

a large scale. Note that recent technology advances have significantly improved the temperature resolution of relatively cheap uncooled IR versions to the point where it becomes sensible to investigate their applications to the IR face recognition field, which is the focus point of our study.

In the initial phase of the study, an image acquisition system was designed and built using an uncooled infrared camera and started the database collection. Then the images were analyzed using two classic recognition algorithms: (a) principle component analysis (PCA), and (b) linear discriminant analysis (LDA) for our proof of concept study. Results show that the uncooled IR camera has sufficient temperature resolution to allow for discrimination between the subjects contained in our experimental database collected under controlled conditions.



Image Acquisition Set-up

The infrared radiation covers a wide

--continued on page 37

Figure 1. Thermal images taken under complete darkness (left) and under room light (right).

ATTACKING AND DEFENDING COMMUNICATIONS NETWORKS, *continued from page 33*

Simulation

A simulation, using the commercially available software package QualNet, is used to produce descriptive results that can be compared to the prescriptive results of the mathematical programming model. Using several runs of the simulation, we select various sets of network components for shutdown, focusing on those suggested for attack by the optimization model. We find that the difference in residual (post-attack) communications flow between the simulation and the optimization model decreases rapidly as the number of attacks increase to about 3% after three attacks. After only one or two attacks, the difference is 15% to 20% of total desired communications flow. We conjecture that congestion in the residual network has a

greater effect under these conditions, which is why we are currently developing a model that incorporates congestion effects.

Conclusions

From this research, we see that prescriptive modeling using mathematical programming can be used in tandem with simulation to determine optimal physical-layer attack and defense points in a communications network. The techniques used here are most appropriate for larger networks with known topology and traffic patterns, where routing is based on shortest-path principles. With further development, this technique may be another useful tool for finding and addressing vulnerabilities in our cyber-infrastructure.

FACE RECOGNITION SYSTEM USING UNCOOLED INFRARED IMAGING, *continued from page 36*

range of wavelengths from 0.7 to 1,000 μm in the electromagnetic spectrum. The heated objects emit infrared radiation with peak wavelength dependent on its temperature. The average human body temperature is about 310 K and emits primarily in the 8-13 μm wavelength band. This constraint resulted in the selection of the IR-160 uncooled IR camera from Infrared Solutions, Inc., which is sensitive to wavelengths in 8 to 14 μm . The camera uses a 160 EMBED Equation.DSMT4 120 pixel microbolometers array to capture images at 30 frames per second that can be displayed on a video monitor and/or transmitted serially via a RS-232 connection using 8 bits/pixels. The image acquisition set-up is illustrated in

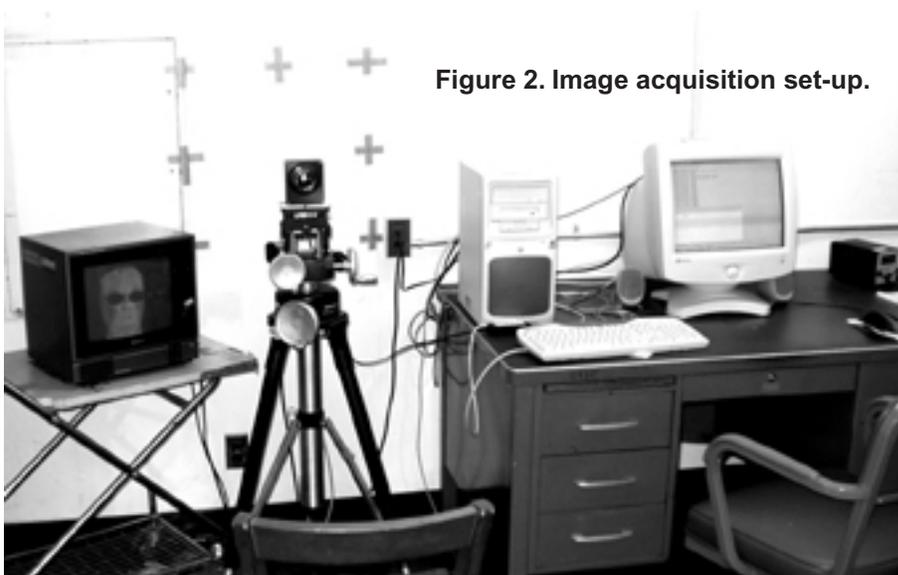


Figure 2. Image acquisition set-up.

Figure 2, where the camera is shown on a tripod, the video monitor is located at the left and the computer collection equipment is on the right.

During the collection of images, each test subject was asked to provide three sets of 10 images each. The 10 images correspond to looking at each of the 9 crosses painted on the wall to introduce tilt and angle variations, as shown in Figure 2, and a tenth image looking at a random location within the boundary of crosses. In addition, variations were also

introduced with different facial expressions in each of the three sets. The first set was restricted to neutral expressions, the second set considered smiling expressions, and during the last set, subjects were asked to pronounce the vowel "u." A total of 420 pictures were taken from 14 adult volunteers, and a sample of the database is shown in Figure 3.

In order to reduce the computation time, the initial 160 \times 120 pixels image size was cropped to include only the face, resulting in images of size 60 \times 45 (i.e.,

vectors of length 2700), as shown in Figure 4.

--continued on page 53



Figure 3 (left). Database sample.

Figure 4 (above). Cropped IR face.

ANALYZING ELECTRIC POWER GRIDS UNDER TERRORIST THREAT

Research Assistant Professor Javier Salmeron, Department of Operations Research

Professor R. Kevin Wood, Department of Operations Research

Professor R. Baldick, Department of Electrical Engineering, University of Texas at Austin

Introduction

The United States' electrical power system is critical to the country's economy and security. The system's vulnerability to natural disasters or physical attacks has been recognized, but this vulnerability has been increasing in recent years because of structural issues, and the threat of terrorist attacks has, of course, become more topical. The goal of this project is developing new mathematical models and optimization methods for robust planning of electrical power grids, focusing on security and reliability with special emphasis on potential disruptions caused by sabotage and terrorist attacks. As an incentive to build these costly, robust networks, secondary economic benefits will be examined too.

Today, the U.S. electric system consists of an interconnected network of more than 6,000 generating units and 800,000 km of bulk transmission lines, thousands of substations with high-voltage transformers, and a huge number of lower-voltage transformers. The network is controlled by more than 100 control centers coordinated in real time. Because current electric networks have been mostly designed following economic principles, i.e., low cost, they lack significant redundancy and minor failures, random or otherwise, can lead to severe system-wide problems.

Potential threats to the system, especially those coming from terrorist attacks, have been recognized in general terms for 20 years or more, but few steps have been taken to improve the situation. Recently, demand growth and increased market competition have led to the system being operated with shrinking reserves. The system is becoming very brittle.

In this project, reasonable tradeoffs between security and cost are being explored. This implies the design of more robust systems, minimizing disruption and its costs, while still making these systems efficient and attractive from an economic standpoint.

The analysis helps address questions such as: "Which substations and other facilities are the most critical to protect?" and "How should they be prioritized?" "What is a reasonable capacity-expansion plan to contribute to increased security?" and "How does this new capacity facilitate competition in electricity markets?"

Estimating Threats

Terrorist attacks are easily conceivable: Most components of

the electrical grid are unguarded and isolated. Terrorists could destroy critical components, which are vulnerable to simple explosives or rifle fire, and incapacitate large segments of the transmission network for weeks or even months. Indeed, electrical power systems have been attacked, or are under continuing attack, in several countries in Latin America, Africa and Asia.

The greatest concerns are substations because they are easy to attack, difficult to repair and critical to system stability if chosen selectively. According to the Office of Technology Assessment, any region in the U.S. could suffer lasting and widespread blackouts if three or more substations were targeted. In fact, loss of a key substation could possibly isolate a region and cause long-term power shortages.

The cost of a blackout and the impact it might have on U.S. society are difficult to estimate. Costs are associated with the interruption of services that require electricity, i.e., almost every activity. Utilities and public utility commissions estimate these costs by assessing the level of economic activity that might have occurred if no blackout had happened agreeing that, in general, outage costs of non-supplied energy can be rated between \$1 and \$5 per kWh. This imprecise estimate does not account for indirect and social costs that cannot be quantified.

Because utilities tend to overlook expensive protective measures when threats are deemed low, they typically plan for one failure (or at most two) to crucial equipment: The usual criterion is to have enough replacement capacity to cope with failure of the largest operating unit or transmission line. Failures range from "normal" failures for which utilities typically have well-prepared response plans to "major" failures which can be attributed to natural causes or manmade causes.

Reliability can be improved through proactive and corrective actions. The former, such as increasing transmission capacity for redundancy or improving the physical security at installations (e.g., by hardening key elements such as building walls and increasing surveillance) are designed to prevent damage, or minimize its consequences. Corrective actions are established to recover normal system functionality in the least possible time. They can include training control-center operators and maintenance patrols for better damage assessment and prompt response, increasing spinning reserves, etc.

--continued on page 39

ANALYZING ELECTRIC POWER GRIDS UNDER TERRORIST THREAT, *continued from page 38*

Model Features and Examples

An optimal interdiction (i.e., attack) model has been devised, subject to limited interdiction resources. “Optimality” implies that the attack causes the largest possible disruption; “limited resources” implies combined attacks on system components, which terrorists might reasonably carry out simultaneously. By studying how to attack power grids, the researchers will ultimately understand how to protect them. By identifying the largest disruptions that might be caused by attacks, the proposed protection plans will be appropriately conservative.

The preliminary interdiction model and an algorithm for its solution have been tested using small- and medium-scale networks drawn from the IEEE’s Reliability Test System (RTS) networks. Given the assumptions made on terrorist capabilities, the algorithm finds the combination of facilities (i.e., generating units, transmission lines, transformers and/or substations) whose destruction would cause the largest or nearly largest disruption in the system at a given point in time. Finding these “target sets,” which in turn suggest the system components most in need of protection is difficult or impossible by simple inspection.

Additional assumptions on the terrorists’ potential are considered. For example, suppose that they may simultaneously and successfully interdict multiple elements of the electric grid depicted in Figure 1 (from IEEE, and referred to as the RTS-One-Area grid). For simplicity of exposition, suppose that the terrorists’ resources can be quantified as six people, and that one person is required to attack any transmission line; two people can attack an electrical bus (therefore isolating all the load, generation and lines connected to it); and three people can destroy the larger substation, which contains four large transformers, located in the middle of the RTS-One-Area grid. In general, the concept of terrorist “resources” can accommodate the available information from intelligence sources. The effect of a set of attacks are measured through the total load that must be shed, i.e., the total amount of demand for electricity that must go unmet.

The algorithm finds many attack plans, from which the following two are chosen to look at more closely: “Plan A” attacks the substation and three selected lines, and “Plan B” attacks six selected transmission lines, as depicted in Figure 1. Plan B sheds more instantaneous load than Plan A, but the total amount of unsupplied energy must be estimated while the effects of the attack last. This entails establishing time lines, or “time regimes,” for repair, and evaluating the resulting load-shedding patterns and their cost, over time. In the example, the 115 MW of additional “short-term” load shedding in Plan B may be negligible when compared to the long-term disruption caused by destroying the four transformers in the large substation.

--continued on page 55

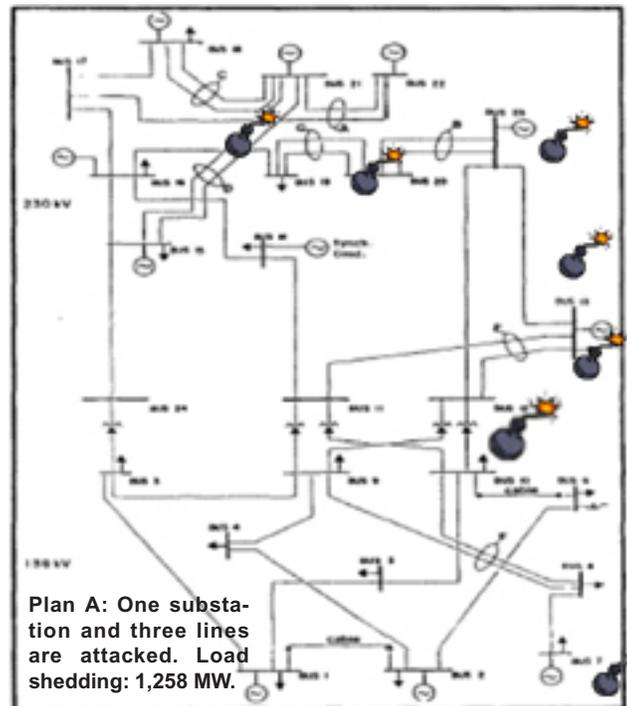
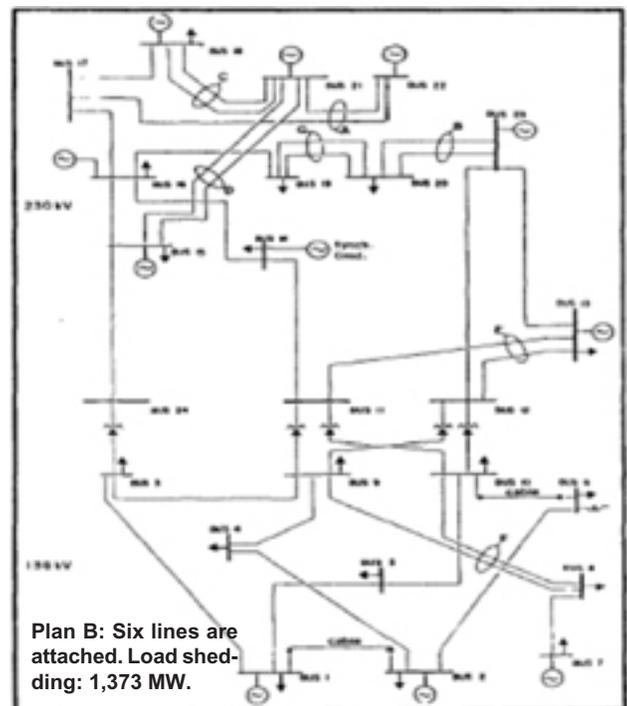


Figure 1. Two interdiction plans on Reliability Test System (RTS-One-Area). Total Load: 2,850 MW (Background illustration source, *IEEE Transactions on Power Systems* (1999)).



VULNERABILITY OF WIRELESS LOCAL AREA NETWORKS TO INTERCEPTION

Associate Professor David C. Jenn, Department of Electrical and Computer Engineering
LT Paul Sumagaysay, United States Navy

Many organizations are choosing wireless local area networks (WLANs) over hardwired networks because of their convenience and flexibility. One challenge in deploying systems that radiate in free space is the possibility of the signal being intercepted by unauthorized users. Even though the power levels involved are very low, a person just outside of a building or in a lobby could conceivably collect sensitive information or possibly even disrupt the computer network by injecting deceptive signals.

Although complex encryption techniques make it difficult for the average person to penetrate the system, the algorithms that are built into the network software have been defeated by knowledgeable hackers. The first step in the hacking process is to gain unauthorized access to network traffic. In many cases this is most easily accomplished by intercepting wireless signals.

Research at the NPS has examined the vulnerability of WLANs to interception and provided some simple steps that can be taken to improve security. Commercially available software was used to predict local mean signal power received at any given point in complex environment, such as the inside of a building. Figure 1 shows contours of signal strength in dBm (where dBm is a decibel relative to a milliwatt reference) at a height 5 feet above the ground for a two story metal composite building. The building footprint is a square, 40 feet on a side, and the WLAN access point is located on the first floor at the + symbol.

Typical WLAN receiver sensitivities range from -94 dBm for 1 Mbps to -85 dBm for 11 Mbps. Therefore, no interception would be possible in the dark blue areas. Note that at the lowest data rate, interception is possible over most of the computational grid, which is 150 feet on a side. Figure 2 shows that the power levels outside of the building have been reduced significantly by moving the access point to the second floor and replacing the standard windows by tinted glass.

The fact that the WLAN is contained inside a closed building gives a false sense of security.

--continued on page 41

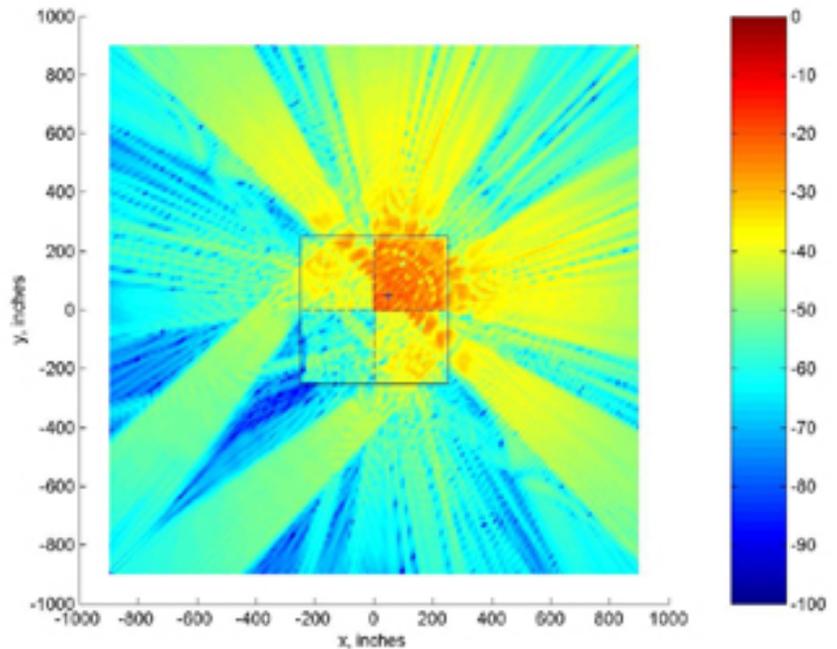


Figure 1. Power levels for a building with metal composite walls and standard glass windows. Units are decibels relative to a milliwatt (dBm). Strong signals passing through the windows are evident.

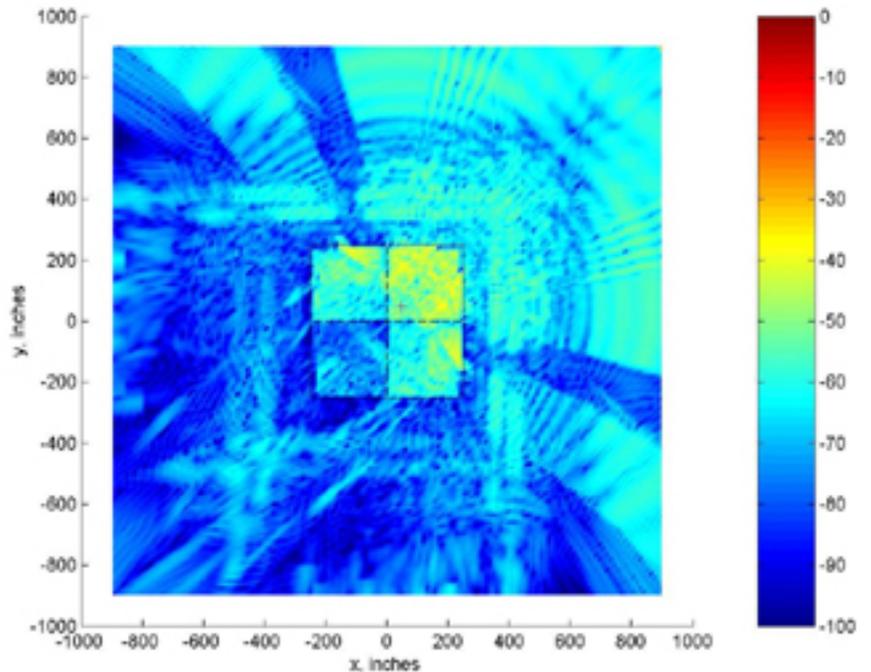


Figure 2. Outside power levels are reduced using tinted glass and moving the access point to the second floor, which reflects signals back into the building.

CONCEALED WEAPONS DETECTION

Research Associate Professor Richard Adler, Department of Electrical and Computer Engineering
Research Associate Professor Jovan Lebaric, Department of Electrical and Computer Engineering

The Concealed Weapons Detection project for Homeland Security Defense is aimed at providing a means of detecting concealed weapons at greater range than existing systems. Existing technology uses near field, magnetically coupled detectors that requires that the target individual be in close proximity to the detector, typically within a foot or less. This does not allow for any advance warning to security personnel. Indeed, several years ago an individual carrying a concealed weapon walked into the U.S. Capitol building. The near field detectors at the entrance sounded an alarm, but the intruder at that time was ready to shoot and he fatally shot two guards and seriously wounded the third, before being shot himself. This incident vividly illustrated the need for an advanced warning of an individual carrying a concealed weapon

approaching a security checkpoint, as did the July 2002 attack at the LAX airport.

This need was confirmed in a meeting with a representative of the U.S. Department of Justice and in a follow-on meeting with the U.S. Secret Service representatives in Washington, DC. To address this need, a new approach to this problem has been developed and implemented. At the time of writing, the proprietary Phase I work has been completed, which is anticipated to be patentable.

The process used tools including self-developed electromagnetics software, as well as the CST Microwave Studio software as a tool for simulation and design. A sample model from simulation is shown at left in Figure 1.

Theoretical results are being validated by experimental measurements in the Department of Electrical and Computer Engineering's Microwave Lab, using the experimental setup shown in Figure 2 above right.

Three M.S. in Electrical Engineering candidates are working with the faculty researchers



Figure 2. Experimental System Setup.

VULNERABILITY OF WIRELESS LOCAL AREA NETWORKS, *continued from page 40*

Many small businesses use WLANs, yet system administrators are not aware of the susceptibility of these systems to interception, or feel that they do not have the resources to tighten security. However, this research has shown that some simple steps can be taken to reduce the probability of interception, such as: locating access points in the most interior building spaces, closing all exterior doors and windows, and using metal blinds or tinting on exterior windows.

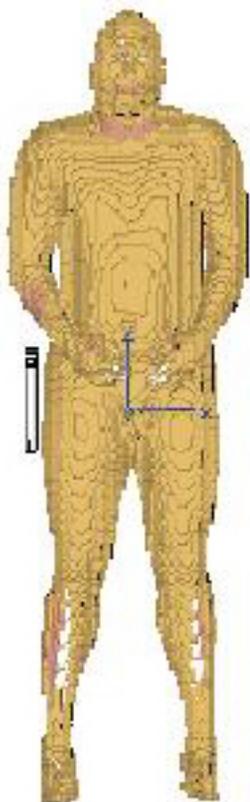


Figure 1. Simulation.

INTELLIGENT SOFTWARE DECOYS

Associate Professor Bret Michael, Department of Computer Science

Professor Neil Rowe, Department of Computer Science

Associate Professor Mikhail Auguston, Department of Computer Science

Associate Professor Doron Drusinsky, Department of Computer Science

Research Professor Richard Riehle, Department of Computer Science

Senior Lecturer Hy Rothstein, Department of Defense Analysis

LCDR Valter Montiero, Brazilian Navy

Maj Donald Julian, United States Marine Corps

Capt George Fragkos, Hellenic Army

LTJG Engin Uzuncaova, Turkish Navy

Mr. Thomas Wingfield, Esq., ManTech Aegis

Research Corporation

The genesis of this project dates back to a series of discussions that took place in the winter of 2001 in the course titled Distributed Operating Systems, in which Professor Michael and his students identified challenges associated with achieving high levels of security in distributed operating systems. Some of the unique capabilities of distributed in contrast to network operating systems, such as managing distributed objects using a global naming space, led Professor Michael to explore how deception could be used in distributed computing to protect critical components of the information infrastructure against the effects of attacks. The research blossomed when Professor Riehle teamed with Professor Michael to create the first prototype of what they call an *intelligent software decoy*, with novel capabilities such as disguising and cloning itself by modifying its contract interface at run-time (via the use of polymorphic argument types). Based on that work, Professor Michael received initial funding from the NPS Institutionally Funded Research (NIFR) Program and the Naval Research Laboratory (NRL) to further investigate his new security paradigm, the results of which were published in [1]. In addition, this work was showcased at the 2001 Eiffel Programming Language Workshop (held in conjunction with the IEEE Conference on Technology for Object-Oriented Languages and Systems) and the Fleet Information Warfare Center's Navy Information Operations/Warfare (NIOW) 2002 Technology Symposium & Exposition, along with an article that appeared in the Defense Information System Agency's *IAnewsletter* [2].

Intelligent software decoys provide a means for automating, to a degree, counterintelligence activities and responses to cyber attacks. The decoys embody what we refer to as *software-based deception* as a means for hardening operational systems against attacks by sophisticated information warriors: these warriors, whether sponsored by nation-states, terrorist

organizations, or organized crime, continuously update their arsenal of custom-designed cyber weapons for use against specific targets of their attacks. In our paradigm, critical units of software are wrapped with "decoying" rules, which are the cyber embodiment of both the policy (including doctrine) of an organization or individual for conducting counterintelligence and applying countermeasures against attackers. The wrappers are placed around critical units of software (e.g., a component or method) to be protected. By critical, we mean units of software that are integral to the continued survivability of an information system and the correct enforcement of the policy embedded in the system.

When a wrapper detects a suspicious pattern of system calls by one or more computer processes, it begins to conduct counterintelligence tasks and initiates countermeasures; pattern recognition is performed at runtime. In contrast to conventional security paradigms, the wrappers, which we refer to as "decoys," conduct counterintelligence by trying to maintain their interaction with suspicious processes, thus allowing for the collection of information about the nature of the processes' behavior. The wrappers respond to requests for service from the processes by applying countermeasures, with coordination of their responses provided by "decoy supervisors." The countermeasures include actions taken to shield the wrapped software from any ill effects of the interaction, and the responses to the processes that are needed to deceive the attacker into concluding that his or her computer processes are successfully carrying out their mission. As new patterns of suspicious behavior are discovered, the database of rules for counterintelligence and countermeasure actions is updated via machine-learning techniques so that the decoys can adapt to the defend against newly discovered types of attacks. Our initial architecture for intelligent software decoys was introduced in [3].

Homeland security within the United States encompasses, among other things, the protection of public and private cybernetic property against espionage and sabotage, especially if such a compromise would have a significant adverse effect on the national security of the United States. Like other

--continued on page 43

INTELLIGENT SOFTWARE DECOYS, *continued from page 42*

security mechanisms for protecting information systems, it is likely that cyber decoys will in some instances be misused. In the United States, criminal law provides us with analogies for preventing or punishing improper state use of deception, and criminal and civil law give us a range of tools to use against private actors. However, in addition to states, nongovernmental entities and individuals can employ cyber decoys. During the first phase the project under the aegis of Naval Postgraduate School's Homeland Security Leadership Development Program, Professor Michael and Mr. Wingfield—who is a lawyer and expert in national security affairs—performed a principled analysis of the use of cyber decoys, with the aim of better understanding the absolute minima in terms of customary principles for what might be considered to be acceptable use of deception. We used a particular type of cybernetic property—a public-switched telephone network (PSTN)—to explore societal and legal issues associated with applying deception. The results of this work to date [4] will be presented in May of this year at the IFIP International Conference on Information Security in May of this year; an earlier

paper [5] discusses in detail the four principles of the *jus in bello* as it applies to software decoys and their use in protecting the semantic web—the semantic web as an enabling technology that could be used by the Homeland Security Department as tool to fight terrorism, but the semantic web itself needs to be protected.

During 2002 we made some significant strides forward on multiple technical fronts. We developed a high-level formal language we named CHAMELEON for specifying patterns of suspicious behavior and decoy responses to such patterns; this work will also be presented at the upcoming IFIP International Conference on Information Security [6] and is based to a large extent on the thesis research of one of our students [7]. Our paper contains a detailed case study of how one can specify detection-and-response actions in CHAMELEON based on computations over event traces for a real-life sophisticated attack program. We have begun work on building a compiler to translate specifications written in CHAMELEON into an intermediate-level specification needed by the NAI Generic

--continued on page 44

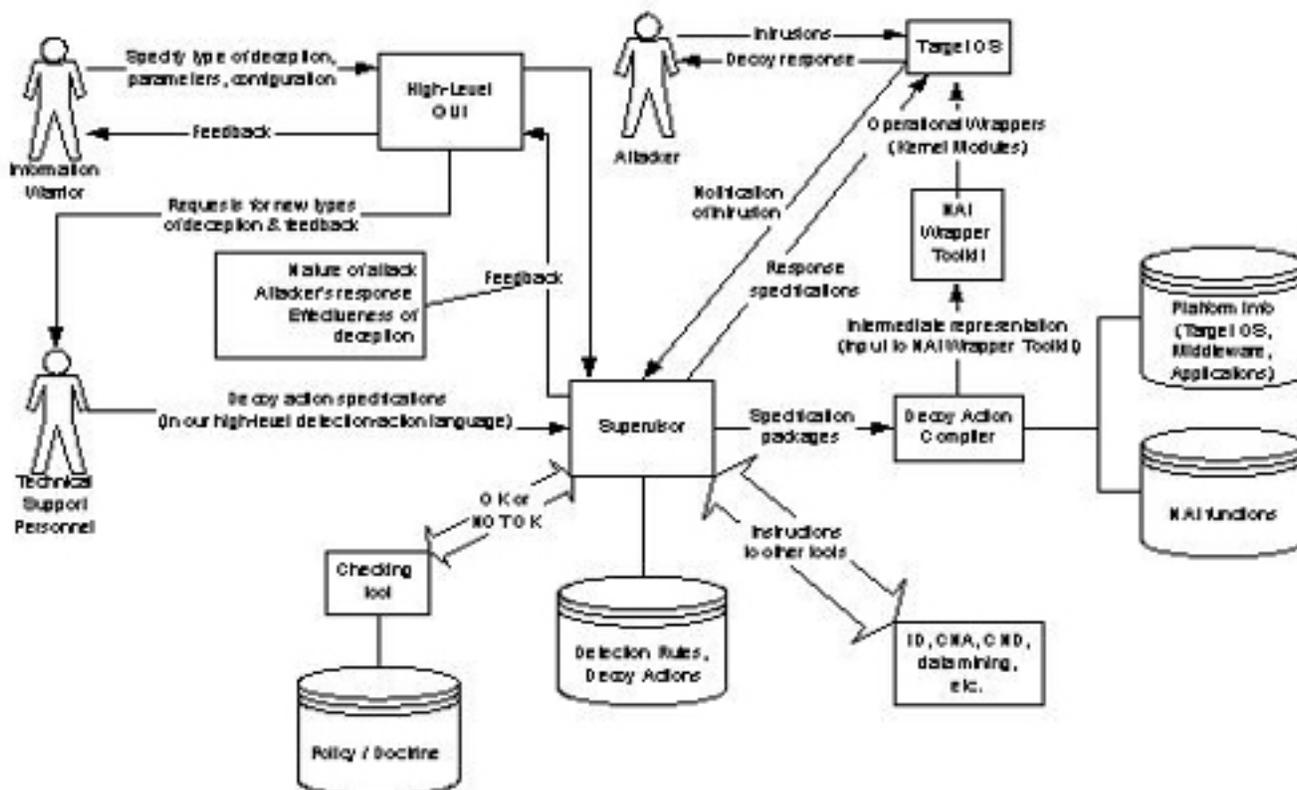


Figure 1. A high-level view of the decoy creation-and-maintenance process as described in [7].

INTELLIGENT SOFTWARE DECOYS, *continued from page 43*

Software Wrapper Toolkit to generate the wrappers around system calls (i.e., kernel modules) which are the low-level realization of the decoys; the compiler effort is spearheaded by Professors Auguston and Michael. Professor Drusinsky is leading an effort to better equip decoys with the ability to reason about the relationship between system and higher level events using temporal logic.

On a related front, Professor Neil Rowe led the effort to explore the use of counterplanning for formulating the most effective set of decoy tactics (i.e., ploys) for a given attack-response situation. We intend to build a theory based on artificial-intelligence planning methods for discrete plans to model possible attack scenarios; see for instance [8]. We intend to enable the decoys or their supervisors to perform analyses of potential perturbations of such plans in order to identify the most disruptive ones, which in turn would be used to construct detailed counterplans that optimize the tradeoff between disruption and ability to deceive the attacker based on plausibility of the ploys used. One of our thesis students working on this project completed a rudimentary study using experimentation with human subjects to test the plausibility of some simple computer-based deceptions involving the use of delayed responses [9]. With the addition to the team of Hy Rothstein, we have made progress toward developing a cyber-version of the theory and principles of military deception; a brief summary of this work appears in [10].

Our initial findings have been encouraging and we will be aggressively pursuing this line of research during 2003. We expect that one of our major contributions to homeland security will be the specification and prototyping of an integrated suite of tools for creating and managing intelligent software decoys, with a high-level interface that is meant for use by intelligence agency watch officers, law enforcement and criminal justice personnel, system administrators, and others involved in homeland security both within the public and private sectors. The high-level user interface will make the low-level details of decoy creation and manipulation transparent to such users. We envision the suite of tools as eventually being used by the Homeland Security Department to coordinate the use of decoys across its administrative domains and the twenty-two agencies from which the department was formed—a formidable challenge in and of itself, as discussed in [11]. We also plan to develop one or more web-based learning modules to teach the theory of software-based deception, along with envisaged

applications to homeland security.

References

- [1] Michael, J. B. and Riehle, R. D., "Intelligent software decoys," *Proceedings: Monterey Workshop on Engineering Automation for Software Intensive Systems Integration*, n.p., (Monterey, CA, June 2001), 178-187.
- [2] Rowe, N. C., Michael, J. B., Auguston, M., and Riehle, R., "Software decoys for software counterintelligence," *IAnewsletter* 5, 1 (Spring 2002), 10-12.
- [3] Michael, J. B., Auguston, M., Rowe, N. C., and Riehle, R. D., "Software decoys: Intrusion detection and countermeasures," *Proceedings: Workshop on Information Assurance*, IEEE (West Point, NY, June 2002), 130-138.
- [4] Michael, J. B. and Wingfield, T. C., "Lawful cyber decoy policy," *Proceedings: Eighteenth IFIP TC11 International Information Security Conference*, Norwell, MA: Kluwer Academic Publishers (Athens, Greece, May 2003).
- [5] Michael, J. B., "On the response policy of software decoys: Conducting software-based deception in the cyber battlespace," *Proceedings: Twenty-sixth Annual Computer Software and Applications Conference*, IEEE (Oxford, England, Aug. 2002), 957-962.
- [6] Michael, J. B., Fragkos, G., and Auguston, M., "An experiment in software decoy design: Intrusion detection and countermeasures via system call instrumentation," *Proceedings: Eighteenth IFIP International Information Security Conference*, Norwell, MA: Kluwer Academic Publishers (Athens, Greece, May 2003)
- [7] Fragkos, G., "An event-trace language for software decoys, Naval Postgraduate School Master's Thesis, September 2002.
- [8] Rowe, N. C. and Andrade, S. F., "Counterplanning for multi-agent plans using stochastic means-ends analysis," *Proceedings Artificial Intelligence and Applications Conference*, IASTED (Malaga, Spain, September 2002), 405-410.
- [9] Julian, D. P., "Delay type responses for use by software decoys," Naval Postgraduate School Master's thesis, September 2002.
- [10] Michael, J. B., Rowe, N. C., Rothstein, H. S., Auguston, M., Drusinsky, D., and Riehle, R. D., "Phase I Report on Intelligent Software Decoys: Technical Feasibility and Institutional Issues in the Context of Homeland Security," Naval Postgraduate School Technical Report, NPS-CS-03-001, December 2002.
- [11] "Homeland security challenge: Make 22 agencies work as one," *Washington Post*, 6 January 2003, E1, E9.

NETWORK MANAGEMENT FOR UBIQUITOUS SURVEILLANCE ENVIRONMENT, *continued from page 7*

to the model are encoded producing an “encode array.” From this encode array an “encode identifier” is produced, which then becomes the key for searching a database of facial images. The ID-2000 software is designed to run as a client-server process. The client node is where the camera (sensor) is, and the encode process takes place. The server holds the database of images, encode arrays and identifiers, and other data related to the image.

- Configuration of ID-2000 in this environment. The ID-2000 software is a lightweight ID package from a relatively new, smaller company. As such, it does not have a wide range of configuration options. Two primary modes exist for this application. Static pictures matched against an enrollment database, and moving video input matched against an enrolled database. After a false start using a Canon ZR10A digital video camcorder (NTSC format), with IEEE 1394 connector (firewire) the team was able to connect the Logitech camera and use the application software to do matching of moving video to a static image stored in the enrollment database.

Network Management Software Configuration

Due to time constraints with this project, very little custom configuration was conducted on the testbed. For the most part, default settings and standard performance monitoring metrics were used in reaching the findings of this paper. The team was unable to develop an experimentation and observation plan for running the application while employing the NMS primarily due to the late arrival of equipment and application configuration problems.

Examination of Telecommunication Management Network (TMN): How Solar Winds Manages Each TMN Layer
SolarWinds is a lightweight NMS. Although it lacks some of the higher layer features that more robust network management packages offer, it does have a fairly diverse collection of tools and modules that allow detailed management at the lower layers. For ubiquitous surveillance, an NMS with functionality similar to SolarWinds would likely be appropriate. Other choices such as HP Open View would have the additional benefit of customizing MIB variables through the use of the Distributed Management Developer’s Kit.

SolarWinds enables the network manager to monitor and manage at a very detailed level. Network layer management is accomplished through the use of multiple tools. Figure 3 is an example of a bandwidth-monitoring tool that can be configured to monitor a particular link.

Network Element management is accomplished through the use of various GUI screens that primarily use IP addresses to refer to the network elements. Figure 4 shows an aggregated view of network nodes and an interface by which to manage them.

--continued on page 46

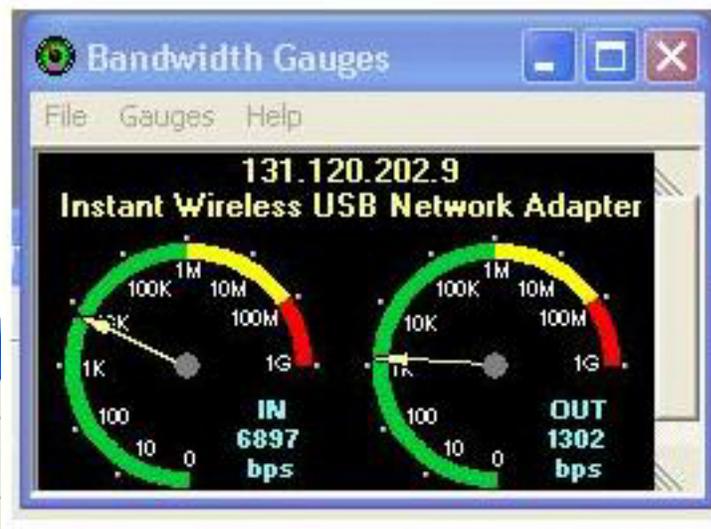


Figure 3. Bandwidth Monitoring Tool.

Figure 4. Aggregated View of Network Nodes and Interface.

NETWORK MANAGEMENT FOR UBIQUITOUS SURVEILLANCE ENVIRONMENT, *continued from page 45*

Network Management at the application level is implicit in SolarWinds capabilities. As an application is running, its effects on the network can be monitored and managed. Additionally, if an application requires supporting services (protocols, ports, etc.) their status can be determined and managed by SolarWinds.

While SolarWinds provides a fairly diverse set of tools to support the management of individual elements in a network, it does not provide direct tools for Service and Business layer management. For Ubiquitous Surveillance in its deployed mode, there will be a need for application and service layer services at a minimum due to the sheer volume of sensors envisioned. It would be desirable to have business layer services as well, although it is our assessment that it is not strictly necessary for successful employment.

For the purposes of the testbed demonstration, the SolarWinds MIB Walk tool was run on each of the nodes operating. The results of the MIB "walk" were captured and an abbreviated set for the client was taken. The discussion and results with regard to management of configuration, fault, traffic, and security monitoring are drawn from these data. There are 11 major groups of RFC1213 MIB variables that are commonly used. Some, such as address translation, are deprecated from MIB I and no longer considered useful.

With the exception of system variables, these groups are not homogenous with respect to the management functions of the NMS. Each has variables that are used for configuration, traffic management (performance), and fault management. Security is not an inherent function of individual variables, although significant work is being done in this field to utilize them as such. For each of these network management functions, a representative sample of MIB variables was selected, examined, and the findings presented. The presumption was made that these variables are used by SolarWinds as part of network management although no direct link could be established between the variables and the output of the SolarWinds system.

Configuration Management Variables/Group

Configuration management is a broad concept that covers many different facets of the network model. It can refer to a particular device's location, what services are enabled/disabled, what actions are pre-set, etc. For each of the testbed nodes, there were literally dozens, if not hundreds, of MIB variables that related to configuration. A representative sample of these is described below, illustrating the type of MIB variables that

are used for configuration by the NMS.

The RFC1213 "system" group is virtually all configuration variables. There are numerous other configuration variables that are part of other "groups" each dealing with specific layers of the OSI model. The interfaces group consists in large part of layer 2 MIB variables.

It is important to note that most, if not all, of the 9 "groups" listed in RFC1213 (MIB II) and 1060 (MIB I) contain configuration variables. The IP "group" handles layer 3 conditions and had different methods for monitoring performance.

Fault Management

Fault management is of prime concern in a ubiquitous surveillance network. If the network is to be relied upon it must be fault tolerant and have robust fault handling features. Fortunately this is a strength of SNMP and its associated MIB variables (both MIB II and proprietary). While the current implementation uses fault detection and reporting, there is current research in this area using intelligent agents to do fault prediction based on subtle network changes, and fault analysis using replicated MIBs to record the values of "crashed" network elements.

Traffic Monitoring

The term "traffic monitoring" is fairly broad and can include elements of both fault and security management. It is therefore examined here with a narrower focus--just Performance Management. Performance management considers factors such as network throughput, response times, line utilization etc.

In a heterogeneous network such as the one described in the scenario, there will likely be multiple transmission protocols running on multiple types of vendor equipment. As a result, the MIB variables that are key to monitoring performance may vary somewhat among protocols. This can be compared with the RFC1213 variables found on the server node MIB on the testbed (which are presumably monitored by SolarWinds).

Security Management

Network and systems security is primarily concerned with five areas: authentication, access control, data confidentiality, data integrity, and non-repudiation. Currently, MIB II as defined in RFC1213 has few objects that relate directly to

--continued on page 47

INTEGRATED ASYMMETRIC GOAL ORGANIZATION, *continued from page 11*

blender either as input or a generic space and become connected to other mental spaces. The result is a growing scale-free network of mental spaces. The integration network gets more and more complicated. More and more mental spaces are combined with it as it goes through its process.

Results

The subject matter expert has produced a collection of data that is formatted in a specific way to work with our blender. The subject matter expert has constructed a data set of over 300 items that became known to the subject. Each item

was tracked so that we knew when it became known to the subject. Approximately 20% of this data set has been tagged and packaged by the subject matter expert. That means that for each item the information has been placed in a formatted blended space with connectors extended that represent the type of information contained in the space. Subject matter expert has also produced about 50 kinds of mental spaces that are supported in the form of generic spaces. For each generic space there is an interior structure that describes in very abstract terms that kind of operation or information.

--continued on page 48

NETWORK MANAGEMENT FOR UBIQUITOUS SURVEILLANCE ENVIRONMENT, *continued from page 46*

security or easily lend themselves to security management.

Current research shows that some MIB variables can be used as indicators of particular types of attacks

Most managed security objects (i.e. MIB variables) are implemented by individual vendors of network equipment, rather than relying on MIB II variables. These security objects are frequently found in firewalls or in networking equipment that can perform at least basic filtering such as routers or switches.

The actual implementation and deployment of a ubiquitous surveillance network has numerous obvious security concerns. Not addressed directly in this paper are the vulnerabilities associated with the physical security of the sensors, nodes, and possible physical links that are part of the network. Physical access to any of these points by an enemy is problematic and makes the defense of the network much more difficult.

Aggregated Network Management

From a network management perspective SolarWinds does an admirable job at providing numerous aggregated views of the network that are drawn from the polling of MIB variables. These views represent the network, network element, and limited inference about the application layers of the TMN management model. There appears to be no direct way to determine exactly which MIB variables are used by each performance or monitoring module.

From a military perspective, there exists an imperative to be able to trust the integrity of the system and the outputs of that system. It would therefore be required that the relationship between the application and the MIB variables be disclosed and known.

Dynamics of Monitoring Process, Data Analysis Tasks, and Distribution of Management Roles

For the purposes of the testbed, the dynamics of monitoring the networks is trivial since there are two nodes, both completely physically controlled. The same holds true for the tasks of conducting data analysis and the distribution of management roles. These topics become important when a larger system is considered, such as in a deployed version of the ubiquitous surveillance network.

In this scenario, monitoring should be as automated as possible and data analysis augmented by automated tools. This may require the integration of a decision support system to augment the process. Lastly, the distribution of management roles will strictly be a function of doctrine, tactics, techniques, and procedures, all of which are purely speculative at this point.

Conclusion

The results of this research will provide vital management information for structuring wireless network surveillance and monitoring process by the Nemesis Van operators. One of the major findings is the set of key SNMP MIB management variables that are most critical for security, fault, performance, and configuration management of the wireless networks that include video sensors, pattern recognition applications, as well as mobile and fixed communication nodes. Finally, the results provide the model of step-by-step implementation of COTS network management system, the SolarWinds tool, for conducting the operations at the Nemesis Van NOC. The network operation site assembled on the floor of the GIGA Code Lab will be used as a static NOC working in tandem with the Nemesis Van mobile NOC.

INTEGRATED ASYMMETRIC GOAL ORGANIZATION, *continued from page 47*

The attack generic space described earlier is an example of such a generic space.

Our blending software has produced its first experimental blends. To our knowledge, this is the first example of a computational model based on software agents to achieve conceptual blending. Detailed software requirements and specifications are complete in a design document. Our software consists of about 140 classes of Java code, 25 of which are part of the human interface (called a GUI). IAGO's human interface will support the following operations:

- Animated visualization of the process of combining inputs to form blended spaces.
- Visualization of networks of the blended spaces (integration networks).
- Textual trace of the information elements produced in the new blends.
- Ability to examine new blends as they are produced.
- Support for collecting blends linking behavior and decisions to a sequence (string) of blends.

Limited funding has brought IAGO to the point where after six months of effort we are able to demonstrate that computational blending is possible and that multi-agent software blending can be applied to support the anticipation of subject behavior.

Methodology

Our computational model of blending results from a combination of multi-agent system techniques. These include tickets, connectors, composite agents, and networks. A ticket consists of one or more frames. Each frame contains an operation or information item that has a specific type. In IAGO there are two types of tickets – one that contains data and one that contains information about operations. The data tickets have connectors extended to describe to the outside world – the world outside the ticket – what the frames contain. The active or operational tickets contain the steps or sequences of operations. Connectors are based on an analogy with the way receptors and control work in biological cells. In the software world connectors have the following operations. They can be extended which means that their type information is known outside of the agent or they can be retracted which means that type information is pulled back inside the agent. An extended connector is waiting for a complementary or matching connector. When two connectors match, the operation is called a connection. A connector consists of a head part with type information and a tail part

of a ticket. When two connectors match, the corresponding tickets inside the two agents execute so the operational tickets begin to execute. In our blending example a connector match may link an input space in the input 1 position with the blender. The ticket execution inside the blender causes new connectors to be extended at the generic space and input 2 positions. A cascading sequence of connectors is extended as the blending process continues. Agent techniques at NPS have focused on composite agents that have interior sub-agents. The motivation is to create software agents that move in the direction of biological cells in terms of their autonomy and coordination with each other. Agents form networks through the connection process. When two agents have successfully matched their connectors, that connection is converted into a persistent link. The result is a growing network of agents. By basing the links on the connection process, our multi-agent system is able to satisfy the two requirements for forming scale-free networks: incremental addition of links and preferential attachment of links. We mean preferential in terms of the intent or goals of the agents that have formed the connection so that the application level intent is what is guiding the construction of the network links.

Conclusion

The first phase of IAGO has shown that MAS computational Model can achieve software blending. This blending process has produced new mental spaces from input streams collected from research into the behavior of a subject involved in asymmetric warfare. First phase software demonstrates that comparisons may be made between the behavior of the real subject and decisions that follow from the computational model. The Blends produced in the subject model yield insight into the subject's conceptual context for behavior.

We are now planning the next phase of IAGO work, a year-long project seeking to build an application test bed that will place software blenders in the input data stream created by our Subject Matter Expert. This step of the project will integrate the human interface GUI and software blenders so that we can conduct quantitative work at an application level. At this point IAGO will support exploration and experimentation with the conceptual context of a modeled subject.

IAGO has extended the Autonomous Software work of the MOVES Institute. Software Blending opens new possibilities

--continued on page 50

DEMONSTRATION OF LINKED UNMANNED AERIAL VEHICLE OBSERVATIONS, *continued from page 21*

are typical in weather factors generated by any atmospheric model. The WOCSS-derived trajectories had to be validated by observations from an in situ collection of wind speed, direction, and temperature. A basic issue being addressed in the demonstration was whether assimilating the very latest observations within the region of the plume adds enough

information to the best mesoscale vector wind profile and turbulent mixing estimates to justify the additional expenditure UAV time and resources.

In the demonstration mode, a data collection/calibration/validation campaign was mounted on the boundary layer vector wind and turbulence-controlled mixing. Data collection

was performed at the demonstration site. The collection was done with 3 ground-stations and one Rawinsonde system to apply to the time varying 3-D description (i.e. 4D) of the test volume. The ground-station systems operated continuously during the entire time collection period with sensors listed in Table 1. The Rawinsonde system (Table 2) was used at scheduled times to collect profiles of vector winds, temperature, and humidity at pressure levels.

The continuous ground-based measurements, schedule driven vertical profile measurements, provided measurements of the time and space separated atmospheric parameters that control dispersion and are required to initialize numerical models. The field collected data were those used to evaluate the suitability of and to correct the atmospheric forecasts as well as to update the toxic plume sampling and response strategy. With ground stations as well as sensors mounted aboard small unit deployed portable UAVs, everything just mentioned would be available in an operational mode.

To accomplish the in situ ground based continuous measurements, three portable instrumented meteorological (Met) towers were installed on 2 October 2002 and in continuous operation until removed 5 November 2002. The tower designation and location, relative to the runway, are:

- West Tower (SMOKE 1)
- East Tower (SMOKE 3)
- North Tower (SMOKE 2)

--continued on page 50

Parameter	Instrument	Installation Requirements	Physical Description
Wind Speed	RM Young	Instruments mounted in well exposed location for good air flow characteristics	Instrument Assembly weighs 10 pounds measuring 2'x3'x6" mounted on 10 ft mast.
Wind Direction	Wind Monitor		
Air Temperature	Rotronics Temp/ RH Probe		
Relative Humidity			
Data Logger	Campbell Scientific CR10X	Data logger mounted near AC power, within 100 ft of Instrument Mast	Data Logger Assembly weighs 20 pounds and measures 12"x14"x6"
Monitor	Laptop PC	PC located in operations space within 100 ft of Data Logger	Requires about 2 sq ft desk space

Rawinsonde System (1)		Installation Requirements	Physical Description
404 Mhz rawinsonde Antenna		Antennae mounted high with good exposure	6 in dia x 5 ft typically rail mounted on 4 ft x 2" nominal dia. pipe
GPS rawinsonde Antenna			3" dia x 2" high rail mounted on 1" dia pipe
Rawinsonde Receiver		Rawinsonde Receiver and Monitor occupy approx 24"x 48" desktop space	MRS Receiver Weighs 70 lbs 18"x18"x24"
Rawinsonde Monitor	Laptop PC and Printer		PC ~ 5 lbs Printer ~10 lbs
Rawinsonde Expendables	Rawinsonde Kites & accessories	Storage Required approx 10 cu ft. in operations areas Kites and accessories up 6 ft in length	
Balloon Launch Shelter		Located in exterior operations area	6 ft DIA x 4 ft high
Helium			2-5 cylinder storage near launch shelter
Operations Support: Spare Parts		Stowed unless failure	200 lbs, 20 cu ft and Tools

DEMONSTRATION OF LINKED UNMANNED AERIAL VEHICLE OBSERVATIONS, *continued from page 49*

With regard to the location at McMillan Field demonstration site at Camp Roberts, the runway is oriented from SE to NW with a taxiway and hanger on the S side of the SE end, Fig 1. Smoke 1, the west Met tower, was located about 50 feet south of the NW end of the runway. Smoke 2, the north Met tower, was located on a hill several hundred feet North of the midpoint of the runway. Smoke 3, the east Met tower, was located about 50 feet north of the SE end of the runway

The towers were instrumented (Table 1) for true vector wind (speed and direction reference to true North), air pressure, air temperature and humidity with identical sensors except that the West and North towers (SMOKE 1 and SMOKE 2) have temperature and humidity sensors at one level only whereas the East tower (SMOKE 3) has temperature and humidity sensors at two levels. The sensors were sampled at 1 Hz and the output averaged over a two-minute interval.

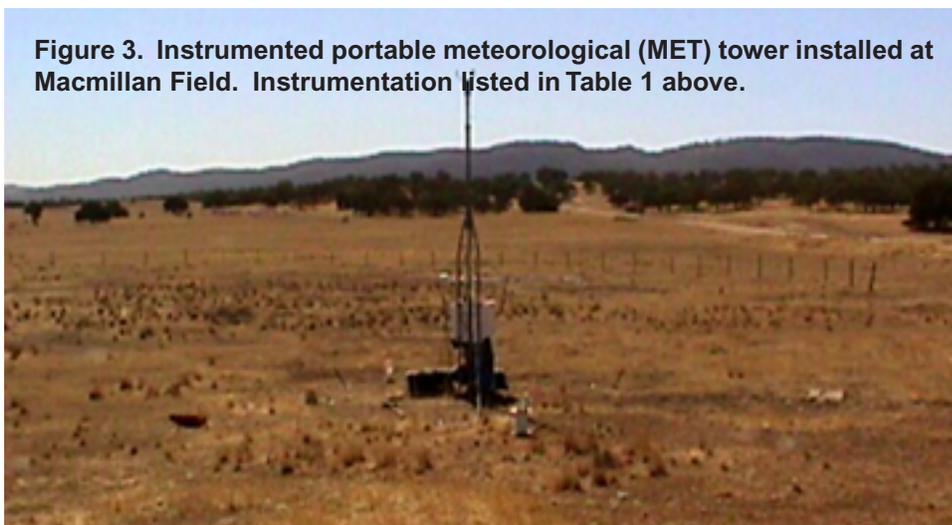


Figure 3. Instrumented portable meteorological (MET) tower installed at Macmillan Field. Instrumentation listed in Table 1 above.

INTEGRATED ASYMMETRIC GOAL ORGANIZATION, *continued from page 48*

for multi-agent systems. Software Blending produces bi-directional Integration Networks. This produces three important consequences. First, agents with this capability may go beyond working with remembered facts to produce new knowledge that is connected and linked to their intent and to their past. Second, when these agents move forward along their Integration Networks, producing new blends from previous knowledge, they begin to know what they know. And conversely, a different process in the agent can move back from the latest blends to earlier mental spaces to produce new blends that contain knowledge about how the agent knows what it knows.

By combining Composite Agents, multi-agent systems, Connectors, and Integration Networks, the first phase IAGO project has brought us to the prospect of building cognitive agents that can extend their Conceptual Blends based on new experience, a capability that will allow them to answer the question, "What are you doing?"

Up/down and balloon tethered rawinsondes were launched from a site near the mid-point of the runway at times before, during, and after UAV sampling. With up/down rawinsondes, data is received from the sonde both during a balloon-ascend and a parachute descent. This provides a better characterization of low altitude atmospheric conditions than with an ascending rawinsonde. It also, provides a three dimensional description of the fields since location is known due to the GPS or Loran navigation inherent in the vector wind determining component of the system. The spatial separation of these profiles will depend on sonde trajectories due to the ambient wind encountered.

The sonde and its parachute were released from the balloon using a timer-release mechanism. The timer was set to release the sonde at an altitude of about 1 km for the first launch of each day, at which point it descended by parachute back to the surface. This height was more than ample to characterize the low altitude atmospheric conditions affecting dispersion and for evaluation of the mesoscale model. Release heights of following rawinsonde flights were set based on an analysis of the profile data from the previous sounding. Additional balloon-borne (tethered) rawinsondes profiles of the near-surface atmosphere (up to about 50-m) were performed throughout the collection as weather and time conditions permitted. These kite-borne sondes should provide a direct measurement of the near surface thermal structure, and thus details of the buoyancy influenced dispersion. The mesoscale models address properties at these scales.

The UAV weather (met) observations for model appli-
--continued on page 51

DEMONSTRATION OF LINKED UNMANNED AERIAL VEHICLE OBSERVATIONS, *continued from page 50*

cation with regard to spatial and temporal accuracy were evaluated. Meteorological observations from the UAVs that directly impact the atmospheric modeling effort are wind speed, direction, temperature, location (altitude, pressure, and latitude/longitude), and time (UTC). However, the primary one is wind speed and direction. The sampling frequency of the UAV is far beyond what is useful for a modeling comparison; so temporal averaging of the observations was required. Tolerable errors in observations of the atmospheric parameters were considered to be 1.0 m s⁻¹, 1.0 °, 1.0 K, 5.0 m, 1.0 millibar, 0.005 °, and 5.0% for wind speed, direction, temperature, altitude, pressure, latitude/longitude, and relative humidity, respectively.

UAV Instrumentation, Data Collection and Processing. Figure 4 represents the planned architecture for the UAV – ground station hardware. Preparation and testing for the demonstration was based on this set-up. The UAV was the Bai Tern (renamed a *Frog*) with 10.5' wingspan and 75 pound maximum takeoff weight. The data was collected by the onboard data acquisition system and transmitted to the ground station via a pair of serial RF modems. In operational modes, the Data Acquisition and Processing Computer on the

ground will do all the necessary data processing to provide the Meteorology Code with the rewire data message, averaged over a pre-specified time interval. For this demonstration, the aircraft was flown by the UAV pilot. Additional guidance cues to the pilot will be developed as necessary.

UAV Demonstration Results

The UAV principal eventual role in this project will be to both map the effective plume dispersion in the atmosphere and provide the wind estimation for the prediction of Chem/Bio agent dispersion. The present role was to make meteorological observations that directly impact the atmospheric modeling effort: wind speed, direction, temperature, location (altitude, pressure, and latitude/longitude), and time (UTC). A one- to two-minute average of atmospheric observations will be sufficiently useful for ingestion into the models.

The UAV results of significance in this demonstration relate to wind comparisons. There are few types of data that determine spatial position of the UAV that is collected for the wind estimation purpose. Data of an airframe is represented by an air velocity and angles of attack and sideslip. Data measured in a body frame by the IMU sensors is represented

by the accelerations, angular rates and magnetic vector variations. GPS data provides direct measurements of the coordinates, ground velocity and ground-tracking angle that are required for wind estimation model.

The wind estimation model has been implemented in a Simulink environment. Real-Time Workshop tool provides an ability to execute this model in a remote computer in real time.

Conclusions

The atmospheric mesoscale model results showed promise in capturing the diurnal evolution of near surface temperatures that drive the local circulations in the warm season. The model consistently underestimated the daytime heating at the ground and yet maintained a reasonable wind and atmospheric stability forecast. Trajectories based on model forecasts showed a reasonable path for the

--continued on page 52

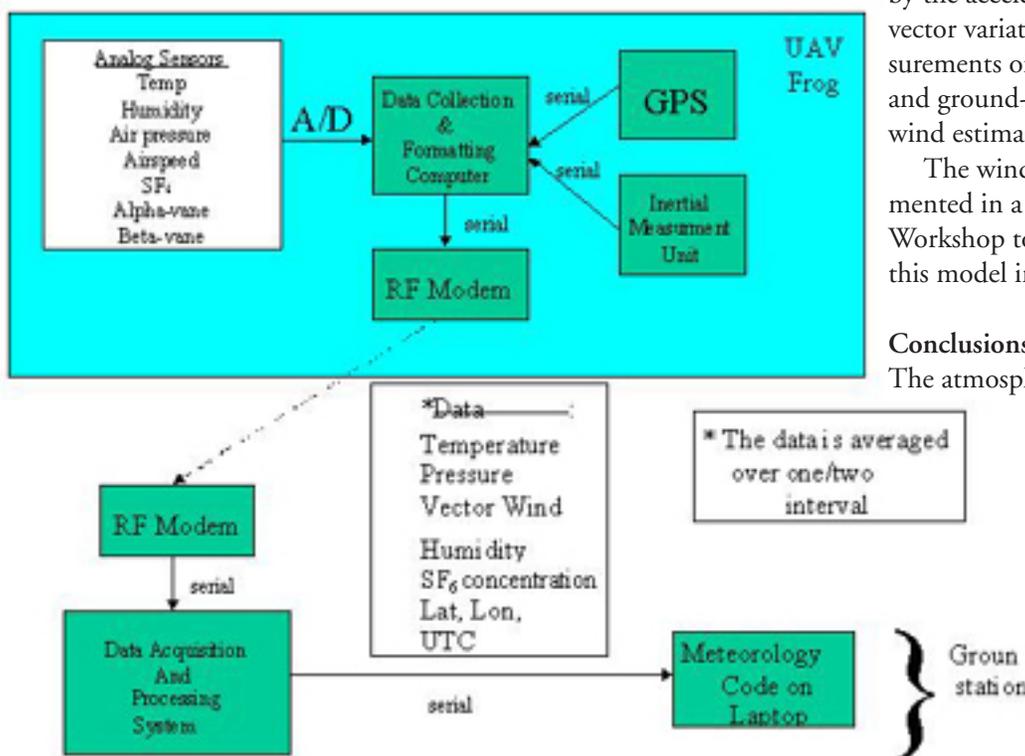


Figure 4. FROG Hardware and Connectivity.

INTEGRATION OF UNMANNED AERIAL VEHICLES AND NAVAL SPECIAL WARFARE OPERATIONS, *continued from page 31*

coordinates). This location was then plotted by the C2 element. Only one data point could be collected for each force (IR strobe).

While all specific MOEs could not be evaluated due to the limitations placed on the experiment, enough data were gathered to demonstrate or infer a positive impact from the use of UAVs. Positive target identification will require more sophisticated equipment, but even the simple IR strobes used in this LOE could help improve target identification if used creatively. Force protection could be greatly enhanced if the low-light camera were replaced with a thermal-imaging camera. The unique IR strobe placed on the red force during the LOE represented this capability and greatly enhanced force protection simply by knowing the location of any enemy personnel within the op area. The average SA differences for the flights conducted with the UAV were much lower than the average SA for all other forces without the UAV. A direct improvement to situational awareness for the C2 element can be seen in Table 2.

This research demonstrated that the use of an inexpensive, small UAV carrying, in this case, a low-light camera and simulated communications relay capability, launched by rear echelon personnel, flown by onboard autonomous avionics to prescribed and changeable waypoints, emitting live video feeds to both the SEAL platoon in the field as well as the C2

element in the rear, proved to have a definite positive impact on the combat effectiveness of NSW forces. While the experiment did not come to full fruition, much data was collected, and analysis of that data led to the following conclusions:

NSW forces don't need, nor do they desire, to be burdened with the requirement of launching or flying the UAV. The concept of the TOC

located at the Forward Operating Base (FOB), launching the UAV for the inserted NSW patrol, has been proven to be valid concept within an 8km range. This range will surely increase

--continued on page 53

Table 2. Situational Awareness Data

<u>Non-UAV Data:</u>	
Blue Alpha 04NOV	7.1
Red Alpha 04NOV	25.0
Pilot Alpha 04NOV	2.8
Blue Bravo 04NOV	3.1
Red Bravo 04NOV	Unknown!
Pilot Bravo 04NOV	2.8
Blue Alpha 05NOV	6.7
Red Alpha 05NOV	Unknown!
Pilot Alpha 05NOV	3.0
Blue Bravo 05NOV	6.6
Red Bravo 05NOV	Unknown!
Pilot Bravo 05NOV	1.1
<u>UAV Data:</u>	
Blue Alpha 05DEC	2.0
Red Alpha 05DEC	1.0
Pilot Alpha 05DEC	0.0

DEMONSTRATION OF LINKED UNMANNED AERIAL VEHICLE OBSERVATIONS, *continued from page 51*

given large-scale conditions but were not verified. Future work would include incorporating observations into the model initialization to correct for the cold daytime temperature bias and examine the impact on successive temperature and trajectory forecasts. Another aspect worth future exploration is the quality of the model forecasts over a broader range of meteorological conditions, validating model performance for cold as well as warm season conditions.

Linking WOCSS with the atmospheric mesoscale model forecasts showed no significant improvement in wind forecasts when compared to the mesoscale model wind forecasts alone. This is an artifact of the test site being located in an open flat basin, where WOCSS essentially acts as an interpolator of the larger-scale weather information. An ideal future test would take place at a site having peaks and valleys unresolved by the coarse horizontal grid spacing of the mesoscale model. Linking WOCSS to the trajectory visualization code revealed

serious shortcomings in the estimate of the vertical wind component that needs to be improved for future tests. Another avenue of future work will be to examine how incorporating actual observations into WOCSS will impact WOCSS-derived trajectory forecasts.

Overall the demonstration proved the feasibility of linking a coarse grid mesoscale model to a fine scale diagnostic wind model for producing fine resolution forward and backward trajectories. As mentioned above, several challenges were noted which will provide future research opportunities to improve on the mesoscale model- diagnostic wind model methodology as a tool for defending against ChemBio weapon attacks. Another very important aspect of future work is the actual transition of WOCSS and the HYSPLIT visualization/ trajectory code to a laptop for a portable capability. This study demonstrated that it was possible to transition to the field Laptop computer.

FACE RECOGNITION SYSTEM USING UNCOOLED INFRARED IMAGING, *continued from page 36*

Face Recognition Schemes

Numerous classification schemes have been reported in the face recognition literature. Classical and widely used approaches are based on eigenface (Principal Component Analysis) and Fisherface (Linear Discriminant Analysis) concepts and/or their variants [1,4]. These schemes are designed to linearly project the image information onto smaller dimensional spaces, where discrimination operations are conducted. Recent results reported by Selinger and Socolinsky show that an LDA-based approach has better classification rate than the PCA for cooled thermal imagery [2], similar to results observed for visible imagery data.

Recall that the goal of the study was to investigate whether face recognition schemes may be applied to *uncooled* IR imaging data with success. As a result, two basic linear PCA and LDA projection schemes were implemented with the long-term goal to use them as benchmarks against more sophisticated schemes in the currently proposed follow-on study. Figures 5, 6 and 7 summarize the basic idea behind the overall face recognition approach implemented: the design

(training) stage, and the decision (testing) stage, respectively. The dataset is split into two portions: training and testing datasets, where the training set is applied to design the classification algorithm, while the testing set is used to test the algorithm classification robustness. Cropped images of size 60×45 are reshaped as one-dimensional vectors of size 2700×1 . Figure 5 shows that reshaped training vectors are stacked column-wise to generate a data matrix of

size $2700 \times N$, where N represents the number of images in the training set. Next, PCA or LDA-based dimension reduction schemes create the projection matrix used to extract the class-specific features needed for the classification step.

Figure 6 presents a three-class training case, where the training data is split into three class-specific subsets. Next, PCA or LDA-based dimension reduction schemes are applied to extract the class-specific features, shown on the feature space as regions C_1 , C_2 , and C_3 , respectively. Finally, each class is represented by its class-specific projected data centroid.

--continued on page 55

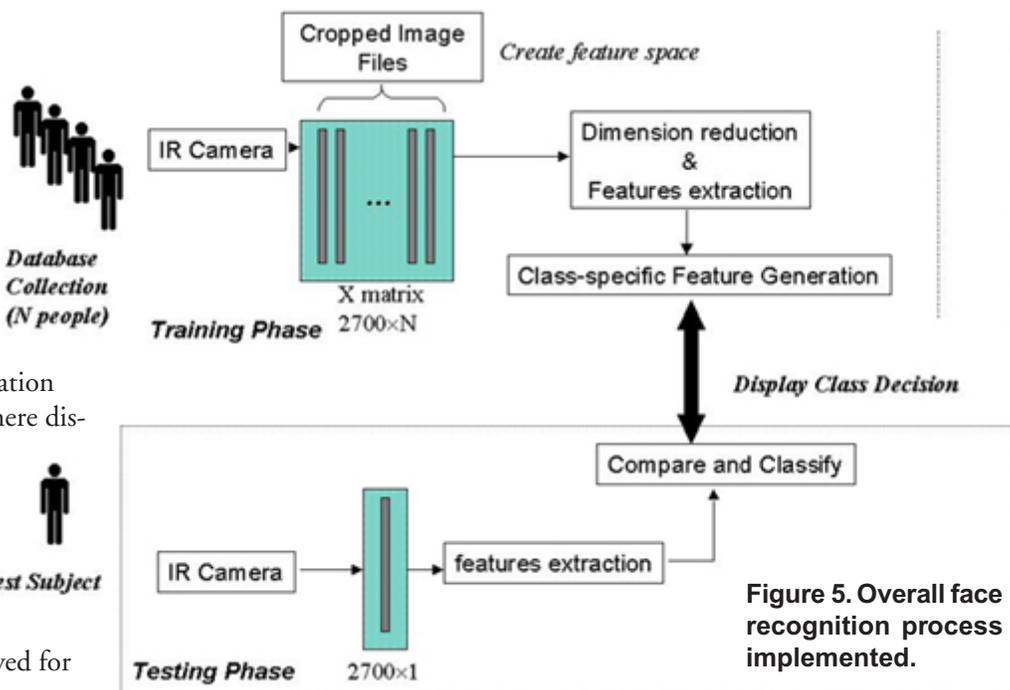


Figure 5. Overall face recognition process implemented.

INTEGRATION OF UNMANNED AERIAL VEHICLES AND NAVAL SPECIAL WARFARE OPERATIONS, *continued from page 31*

as video and communications improve.

Viewing a video feed in the field, during a foot patrol, near a target area may not be as advantageous as having a C2 element (dedicated to viewing that feed) relay the information over a communications net capable of maintaining constant communications. (Note: the C2 element in the LOE was solely dedicated to observing and communicating with the single NSW element in the field).

The ability to track blue forces on the ground with a small tactical UAV has been demonstrated. The IR strobes utilized for the LOE purposes were not clandestine enough for operational use during special operations, but this limitation can be easily overcome.

NSW forces can quickly adapt to the use of these new technologies. Developers of UAVs and their supporting technologies can benefit from feedback from operators in the field conducting LOEs.

FACE RECOGNITION SYSTEM USING UNCOOLED INFRARED IMAGING, *continued from page 53*

During the testing stage, testing datasets are projected into the feature space, using the projection matrix defined during the training stage, and their features compared against each class-specific centroid. Various class decision algorithms exist, and the minimum distance classifier was selected, where final class decision is made by selected for class with the centroid closest to the projected testing set features, as illustrated in Figure 7.

This proof of concept study showed that the uncooled IR image resolution is sufficient to discriminate between the 14 subjects currently enrolled in the database. Figure 8 presents overall classification results obtained using a 60/40 cross-validation set-up and 1000 simulations, where the contribution of the top four eigenvectors is removed from the PCA projection matrix to improve the algorithm robustness to intensity variations. Results show better performances for LDA than PCA based recognition schemes, as expected from their definitions. Further details may be found in Pereira [3]. Extensions to the current work include expanding the database, and investigating non-linear kernel-based projection schemes for classification applications.

Bibliography

1. F. Prokoski, "History, current status, and future of infrared identification," IEEE Workshop on Computer Vision Beyond the Visible Spectrum: Methods and Applications, Hilton Head Island, SC, 16 June 2000.
2. D. Socolinsky, L. Wolff, J. Neuheisel, and C. Eveland, "Illumination Invariant Face Recognition Using Thermal Infrared Imagery," Computer Vision and Pattern Recognition (CPVR), Kauai, HI, December 2001.
3. D. Pereira, *Face Recognition using Uncooled Infrared Imaging*, Electrical Engineer Thesis, Naval Post-graduate School, December 2002.
4. R. Duda, P. Hart, and D. Stork, *Pattern Classification*, 2nd Ed., Wiley Interscience, 2001.

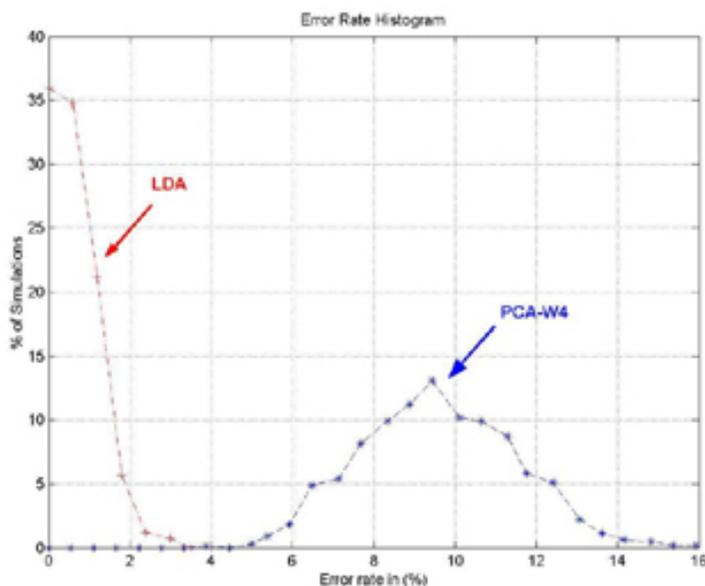
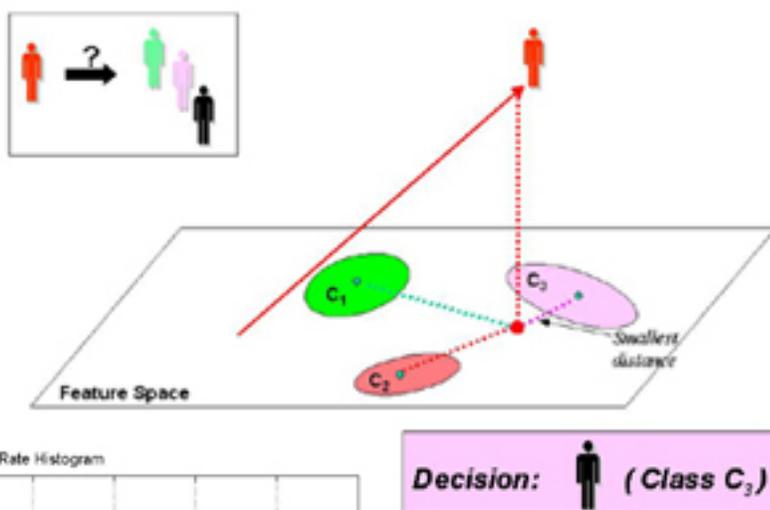
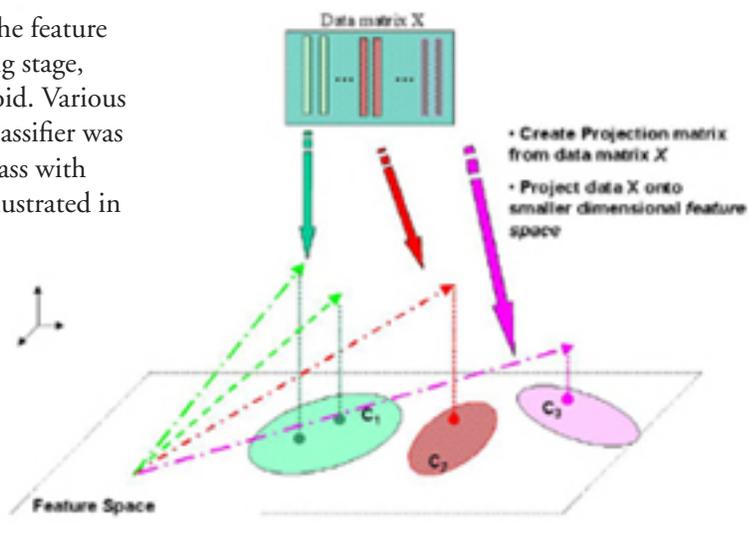


Figure 6 (top). Training (decision) stage.

Figure 7 (above). Testing (decision) stage.

Figure 8 (left). Overall classification performances for LDA and PCA (without the top four eigenvectors) implementations; 60-40 cross validation, 1000 simulations from [3].

ANALYZING ELECTRIC POWER GRIDS UNDER TERRORIST THREAT, *continued from page 39*

Research is currently dealing with a time-regime representation of power restoration. It is assumed that, in the first few seconds after the attacks, all self-protective systems work properly, and evaluate the cost from that moment until the power is fully restored to normal. While lines and minor equipment can be repaired or replaced in days, or at most weeks, typical practice in the electric utility industry is to have only limited spares for expensive transformers. One issue anticipated is representing the tradeoff between the cost of owning additional spares and the reduction in repair time such spares would provide.

Regarding computational efficiency of the algorithm, an optimal solution can be found (optimality verified through other means) to the aforementioned interdiction problem in one minute on a 1GHz desktop computer. However, proving that this solution is actually optimal can take much longer. Mathematically, the goal is to characterize exact optimality, or find tight bounds on maximum error. Significant effort is being made to achieve these goals.

Mathematical Aspects of the Interdiction Model

The basic model is viewed, without time regimes, as in Model 1a in Table 1. In this model, $\delta \in \Delta$ represents resource-constrained binary interdiction decisions for the terrorists, and y represents the optimal power flows, generation and load shedding. Remark: Although the original constraints in the inner minimization involve non-linear functions in δ , assume that a proper linearization of the problem is possible, so that the δ 's can be isolated on the right-hand side as shown. The computational difficulty of this model stems from the max-min structure of the problem. The inner minimization is over a polytope that depends on δ . Solution of the inner minimization as a function of δ yields a convex function. Consequently, the outer maximization is over a convex function, which is, in general, computationally difficult. In addition, the domain for δ is a discrete set, which turns the aforementioned convex function into a non-convex non-differentiable one.

Suppose this is extended to three scenarios representing different time regimes. The resulting model is represented by Model 1b in Table 1. This model is substantially larger, and will require the identification of extensive data to be reasonably accurate, and may require the development of new solution techniques.

Ongoing work

The power flow model we use is simplified to a so-called DC representation of the full AC model, which neglects reactive

$\begin{aligned} & \max_{\delta \in \Delta} \min_{y} cy \\ & \text{s.t.} \begin{cases} Ay \leq B\delta \\ y \geq 0 \end{cases} \end{aligned}$	$\begin{aligned} & \max_{\delta \in \Delta} \min_{y_1+y_2+y_3 \geq 0} cy \quad c_1y_1+c_2y_2+c_3y_3 \\ & \text{s.t.} \begin{cases} Ay_1 \leq B_1\delta \\ Ay_2 \leq B_2\delta \\ Ay_3 \leq B_3\delta \end{cases} \end{aligned}$
---	---

Table 1: Interdiction models: without time regimes (Model 1a, left), and with time regimes (Model 1b, right). (Linearization of non-linear constraints in δ is assumed.)

power effects. This entails various assumptions, many of which may be acceptable in the context of security analysis, but more precise modeling may be necessary. For instance, we may also need to model non-linear losses, DC lines (e.g., the Oregon-California DC tie line), transformer tap positions, transformer redundancy and connectivity at substations, capacitors, VAR compensators and synchronous condensers, unit commitment issues in the short-term, post-contingency analysis, etc.

As is normally the case in large-scale models, we need to find a compromise between model accuracy and tractability. The extent to which exact methodologies can be relied upon to solve the problem is limited as levels of decisions are aggregated and new modeling features are incorporated.

An example of the research being performed, it is noted that Model 1a of Table 1 can be converted to

$$\begin{aligned} & \max_{\delta \in \Delta} \min_{y,s} cy + \delta^T B^T P s \\ & \text{s.t.} \begin{cases} Ay \leq Is \\ y,s \geq 0 \end{cases} \end{aligned}$$

where P is a diagonal matrix of penalties which represent upper bounds on dual variables. The inner minimization is now a concave problem in δ and can be readily solved, in theory: The model can be converted to a mixed-integer program and solved directly, if it is not too large. (Note: The conversion just described is typically referred to as "convexification," although it is actually "concavification" in this case.)

However, the penalties represented by P are not easy to

--continued on page 56

ANALYZING ELECTRIC POWER GRIDS UNDER TERRORIST THREAT, *continued from page 55*

define in this complicated power-flow situation: If they are too large the model will be difficult to solve; and if they are too small, an incorrect solution will be obtained, perhaps with no indication that it is incorrect. The topic of “dynamic penalties” is being pursued where small initial penalties are defined and are increased within the branch-and-bound solution algorithm, as needed.

Learning the best way to attack electric grids allows better analysis of how to defend them. However, the first difficulty here is to determine a realistic set of protective measures, or “measure types,” for consideration, from which the optimization analysis can recommend a selected number of specific actions to undertake.

Mathematically, modeling protective measures entails adding a third level in the hierarchy of decisions to be made:

$$\begin{aligned} \max_{p \in P} \min_{\delta \in \Delta(p)} cy \\ \text{s.t. } \begin{cases} A(p)y \leq B(p)\delta \\ y \geq 0 \end{cases} \end{aligned}$$

In the above model, $p \in P$ represents the set of feasible protective measures. Accordingly, terrorists will determine their strategy, $\delta \in \Delta(p)$, and the (improved) electric system

will determine load-shedding patterns after the attack.

Finally, in many parts of the United States today, restructuring of the electricity industry has led to an increased role of wholesale markets for electricity. An important ingredient of successful electricity markets is the availability of sufficient transmission capacity to allow various generation resources to compete to sell energy. The transmission capacity necessary for a vibrant market is typically more than was required in the pre-restructured industry, but in most jurisdictions there has been little transmission construction in the last decade. However, increased transmission capacity, through redundancy, can improve security while allowing greater access by competitors under normal conditions. Establishing an economic incentive for the utilities to create more secure networks may mean that the necessary construction will actually take place without government mandate. Part of the research will extend the max-min-max models to incorporate the value of improved competitiveness along with the value of reduced susceptibility to attacks. In doing so, dealing with how to compare low probability, high cost issues with certainties of protecting costs and new construction costs (which is being expanded to obtain market benefits) is anticipated.

For further information about student and faculty research at the Naval Postgraduate School, contact the Associate Provost and Dean of Research.

Distinguished Professor David W. Netzer
Associate Provost and Dean of Research
Code 09
Naval Postgraduate School
Monterey, CA 93943-5138
Phone: (831) 656-2980
Fax: (831) 656-2038
E-mail: research@nps.navy.mil

Information about faculty and student research is also available in:

* *The Compilation of Theses Abstracts*, a quarterly publication containing unclassified abstracts for

theses submitted for the degrees Doctor of Philosophy, Doctor of Engineering, Engineer, Master of Science, Master of Arts, and Master of Business Administration. This publication is available on-line at <http://www.nps.navy.mil/Research/thesisyr.html>. Copies of NPS theses are archived in the Dudley Knox Library accessible at <http://library.nps.navy.mil/uhtbin/webcat> (click on Thesis Search).

* *NPS Summary of Research*, an annual publication detailing the research projects and publications of NPS faculty. This publication is available on-line at <http://www.nps.navy.mil/Research/researchsummaries2.html>.

To be placed on the mailing list for *NPS Research* or any of the above publications, please e-mail research@nps.navy.mil.