For five days in October 2003, the ISTS Exercise and Scenario Development (ESD) team conducted a mock “cyber war” against America. The Livewire National Cyber Exercise was designed to simulate a prolonged 30-day cyber attack by a sophisticated, well-financed and determined enemy against interdependent infrastructures such as financial markets, utilities and telecommunications. One of the key challenges was developing a realistic scenario in which key decision makers would be fully immersed in a demanding exercise while physically dispersed around the nation, as they would be in a real attack.

Ultimately, the exercise aimed to identify the requirements for a National Cyberspace Security Response System called for in The National Strategy to Secure Cyberspace published by the White House in 2003. With a National Cyberspace Security Response System, analytical and incident response capabilities in various organizations could be coordinated to defend against a cyber attack, mitigate its effects and restore services. As a “discovery event” rather than a tabletop test or evaluation, Livewire was the first of its kind, engaging private sector business enterprises as well as elements of federal, state and local governments. Rather than expose weaknesses or deficiencies as is typical of such exercises, Livewire allowed stakeholders to practice better inter-agency and inter-sector cooperation, repackage new roles and responsibilities, and identify communications and technology gaps.

During Livewire, approximately 300 people from 50 private-sector entities and government agencies in 14 locations around the nation participated. Members of several business sectors identified as critical to the stability of the U.S. economy, as well as key government agencies, explored how both traditional and potential new relationships would be used to resist a cyber attack. These included the energy, finance and telecommunications sectors, federal agencies, and several state and local governments.

Livewire employed a network simulation that modeled the computer networks of the participating entities, allowing for realistic and effective decision-making on the part of the leadership and technical staff of the participants. To protect the assets of the participants, no actual network for any player was involved in any portion of the exercise.

Additionally, Livewire offered opportunity for formal academic research. Assistant Professor Denise Anthony and Rockefeller Post-Doctoral Fellow Eleanor Lewis of Dartmouth’s Department of Sociology are studying the basis for trusted communication between the organizational entities re-sponding to a cyber crisis. Drs. Anthony and Lewis gathered interview and observational data prior to and during the exercise, and are currently examining the email communications data collected from hundreds of Livewire participants. Joining Lewis in the research was Assistant Research Professor of Physics Tim Smith. Drawing upon his background in developing computer systems for large scale physics particle accelerator experiments, Dr. Smith developed the network simulation and presented the results with a paper at the annual SPIE (The International Society for Optical Engineering) Defense and Security Symposium last year.

Also critical to the success of Livewire was the assistance of Dartmouth’s Public Key Infrastructure (PKI) Lab. The PKI Lab developed and implemented secure exercise communications. Because the exercise was web-based and the simulation was distributed over so many locations, it was vital to provide access to all players while maintaining strong security. With the help of the PKI Lab, the Livewire exercise used an ad hoc secure Internet Protocol suite.

Exercise Director Andy Cutts

The Livewire Simulation Room outside of Washington, DC.

The Livewire Exercise Simulates Cyber War

Welcome to the first issue of ISTS Quarterly. This new publication is intended to inform a broad readership about the full range of ISTS activities and opportunities. In this first issue you will find a report on a national cyber attack exercise, Livewire, an account of a New Hampshire Cyber Summit hosted by ISTS; and research on fully human antibodies to protect against anthrax.

ISTS was founded at Dartmouth in March 2000 and has received major funding from the Office for Domestic Preparedness (Department of Homeland Security) and the National Institute of Justice (Department of Justice). The focus of ISTS research is advanced technology to protect the integrity of the Internet, computer networks and other interdependent information infrastructures. ISTS also addresses topics related to bio-terrorism and is developing sophisticated computer-based educational tools for first responders. Currently, ISTS is conducting twenty research projects involving fifty researchers, thirteen faculty representing Arts & Sciences, Thayer School of Engineering, Dartmouth Medical School, and recently the Tuck School of Business, and nineteen students. Since inception, over ninety researchers and fifty-five undergraduate and graduate students have contributed to ISTS initiatives.

ISTS is also a member, and chair, of the Institute for Information Infrastructure Protection (I3P), a consortium of 24 leading academic institutions, non-profits and federal laboratories collaboratively addressing open issues concerning the safety, security and robustness of the nation’s information infrastructure. Details about I3P activities can be found in the section “I3P News,” which will be a regular feature of the newsletter. Information Security and Privacy Center.

I hope you find ISTS Quarterly informative and stimulating. More details about ISTS and I3P activities can be found on the ISTS web site www.ists.dartmouth.edu and the I3P website www.the3p.org.

Martin Wybourne, Executive Director

continued on page 2
The Institute for Information Infrastructure Protection (I3P) is a consortium of 24 leading national cyber security institutions, including many of the premier academic research centers, government laboratories and non-profit organizations in the country.

The I3P was founded in 2002 to uncover critical information infrastructure vulnerabilities and identify and address the most pressing research and development (R&D) needs. The institute’s main role is to help shape a national cyber security R&D strategy, identify, prioritize and address under-funded research gaps, and promote collaboration and information sharing among academia, industry and government.

As part of this mission, the I3P published a national cyber security R&D agenda in January 2003 and continues to work toward identifying and addressing critical research problems in information infrastructure protection.

The I3P actively supports the research community in its pursuit of technical and policy solutions to the most urgent cyber security problems. The institute is developing research programs to gain a deeper, more detailed understanding of pivotal security issues and fund collaborative research projects in areas not sufficiently covered by government and industry R&D. The I3P has launched a fellowship program supporting up to five fellows per year, each based at one of the consortium member institutions, working on research to close gaps identified in the I3P’s R&D agenda. Further, the institute is building an online knowledge base to provide researchers with a forum for discussing their work, as well as finding information on other experts in the field, security events, funding opportunities and security news. The I3P now produces the daily news summary Security in the News, a free, online news service providing up-to-date articles on such topics as cyberterrorism, infrastructure protection and legislation.

College Partners with New Hampshire Officials in Cyber Summit

In November of 2003, ISTS led the first in a series of working meetings to develop a cyber crime and cyber security strategy for the state of New Hampshire. The New Hampshire Cyber Summit, jointly hosted by the New Hampshire Attorney General’s Office and the Provost of Dartmouth College, brought together law enforcement, public safety and academia to preview ISTS research and discuss cyber crime nationally and in New Hampshire.

Speakers at the Summit included New Hampshire Governor Craig Benson, Dartmouth President James Wright, New Hampshire Attorney General Peter Heed (Dartmouth ’72), New Hampshire Deputy Attorney General Kelly Ayotte, Dartmouth Provost Barry Scherr, and ISTS Executive Director Martin Wyboume, as well as several ISTS researchers.

Brodly defined, a “cyber crime” is any crime committed by means of the special knowledge or expert use of computer technology, or criminal offences committed against or with the aid of computer networks. Some examples of cyber crime include: acquisition fraud, child pornography, cyber attacks, identity theft, software piracy and online stalking. Increasingly, investigations, forensics and prosecutions in the cyber domain require unique skills and advanced training to keep pace with the knowledge and resourcefulness of today’s sophisticated cyber criminals.

The Summit began with a technology briefing covering current ISTS research in investigative tools and technologies, detecting network intrusions, discovering digital tampering, designing sensor networks, communication technology for first responders, and preparing and training for responses to terrorist activities. In a closed session examining New Hampshire cyber crime issues, Attorney General Heed emphasized his commitment to develop a comprehensive cyber crime strategy for New Hampshire and expressed his support for Governor Benson’s initiatives to make prevention, investigation and prosecution of cyber crime a top priority. An overview of cyber crime by the ISTS Technical Analysis Group addressed themes of the borderless nature of cyber crime, electronic crime links to homeland security and the economic impacts of cyber crime.

Deputy Attorney General Ayotte stressed the need for a collaborative effort to fight cyber crime, noting that the capability to effectively respond to cyber crime will drive prevention efforts and substantially affect public safety, economic stability and homeland security in the Granite State. The participants plan to meet again in 2004 to develop a strategic plan to address the critical issues raised at the Summit.

© Copyright 2004 Trustees of Dartmouth College
Photography: Joseph Meeling ’69, Jon Gilbert Fox, Doug Hill
Stephen Snyder
Editor: Stephen Snyder
Design: Susan Warner, Dartmouth College Public Affairs

continued from page 1

Denise Anthony

Eleanor Lewis and Tim Smith at the Livewire exercise.

(left to right) N.H. Attorney General Peter Heed ’72, N.H. Governor Craig Benson, and Dartmouth President James Wright at the New Hampshire Cyber Summit, examining cyber crime nationally and in New Hampshire.
Dartmouth Students Sharpen Their Skills at

During any given term, there are often more than 20 Dartmouth undergraduate and graduate students participating in ISTS-sponsored research complementing their fields of study or personal interests. Because the research scope of ISTS is broad, students may take assignments advancing their computer science and engineering studies, expanding their understanding of national security-related public policy issues, supporting improvement of cyber and first responder technologies, or sharpening their analytical skills.

Two Dartmouth undergraduates, Kim Siciliano and Nicholas Ray, helped in the Dartmouth-developed cyber portion of the TOPOFF2 initiative in May 2003. The primary focus of TOPOFF2 was helping emergency response personnel in Washington State and Illinois practice their response to simulated attacks by Weapons of Mass Destruction (WMD), while the cyber exercise tested local, state and federal emergency response capabilities to cyber attacks.

Eric Krupski ’04 was part of an ISTS research group developing tools to help protect the Internet and other large computer networks from malicious attacks. Krupski, a computer science and mathematics major, contributed to developing software that protects web servers from worm or virus attacks and overwhelming traffic. Welton Chang ’05 worked with ISTS’s Technical Analysis Group, focusing on identifying and addressing critical cybersecurity needs for federal, state and local law enforcement. Chang was one of the major authors of a report on the cyber capabilities of several foreign countries.

The Livewire exercise also involved several academic initiatives on the part of Dartmouth College students and faculty. Student interns Geoffrey Stowe ’04 and Joshua Stabiner ’03 worked with the intelligence community to develop the security systems for the exercise and implemented the specialized email system and database the players used. These interns applied their classroom experience in learning the latest in simulation modeling and building in addition to conducting a major training exercise.

Antibody Protects and Treats Anthrax Infection

A pre-clinical study funded in part by ISTS and coordinated by Ron Taylor, PhD, a Dartmouth Medical School researcher with expertise in treating and preventing infectious diseases, was conducted to determine both the minimal amount of a fully human antibody required to protect against anthrax as well as the antibody’s therapeutic activity when given at the time of anthrax inhalation. The antibody, MDX-1303, protected against inhalation anthrax at a dose tenfold lower than previously tested in rabbits treated with the antibody, and reduced mortality even when administered 1-2 days after inhalation, once animals displayed signs suggestive of disease.

Taylor worked with the U.S. Army Medical Research Institute of Infectious Diseases (USAMRIID) and Medarex, Inc. under a Cooperative Research and Development Agreement to research therapeutics for the treatment of anthrax, an acute infectious disease caused by the spore-forming bacterium Bacillus anthracis. The serious forms of human anthrax are inhalation anthrax, cutaneous anthrax and intestinal anthrax.

USAMRIID, located at Fort Detrick, Maryland, is the lead medical research laboratory for the U.S. Biological Defense Research Program. Medarex is a biopharmaceutical company focused on the discovery and development of fully human antibody-based therapeutics to treat life-threatening and debilitating diseases. Tests to determine the efficacy of the antibody using an inhalation rabbit model were conducted at a separate, independent specially-equipped facility in the Midwest.

MDX-1303 is a fully human antibody against inhalation anthrax, the most lethal form of illness in humans caused by the Bacillus anthracis bacterium, and targets a protein component of these lethal toxins known as the anthrax protective antigen. The anthrax protective antigen initiates the onset of the illness by attaching to cells in the infected person, and then facilitates the entry of additional destructive toxins into the cells. MDX-1303 is designed to target the anthrax protective antigen and protect the cells from damage by the anthrax toxins. The results indicated that all doses tested were protective in rabbits exposed to lethal doses of anthrax spores by inhalation. The results also demonstrated that administration of MDX-1303 to rabbits 24 or 48 hours after exposure to anthrax could result in recovery and survival of the animals without the addition of antibiotics. These results support that the MDX-1303 antibody has the potential to be developed both as a prophylactic to protect people at risk of exposure to anthrax, such as first responders or unvaccinated military personnel, and as a therapeutic for patients already showing signs and symptoms of anthrax infection. The finding that the antibody is therapeutic suggests that it has the potential to augment antibiotic treatment, which by itself is poorly effective in symptomatic infection.
ISTS Speaker Series

ISTS brings an array of business, government and academic visitors to Dartmouth for public talks as part of its Speaker Series. Topics range from cyber-security and first responder technologies to the economic impact of cyber and infrastructure vulnerabilities. The goal is to promote understanding, collaboration and dissemination of knowledge about these matters among researchers, and expose students, faculty and other members of the Dartmouth community to the issues, challenges and solutions examined.

Some of the recent speakers included Matt Bishop, Professor of Computer Science, University of California at Davis; Bruce Schneier, Founder and Chief Technical Officer of Counterpane Internet Security; and Rand Beers, former Assistant Secretary of State and Special Assistant to the President for Combating Terrorism (photo at left).

Future talks will focus on science, technology and government; computer security, privacy and electronic commerce; and Internet security technologies.

Grants & Awards

Sean Smith and his Public-Key Infrastructure (PKI) team received $100k from Cisco Systems to launch the Greenpass project. Greenpass applies PKI technology to the challenge of authenticating users of WiFi wireless networks, and allowing authenticated users to delegate network access to visitors.

Andy Cutts and the Exercise and Scenario Development group received a $500k grant from the CIA to help them conduct the Livewire National Cyber Exercise.

George Cybenko and his team won a grant initially worth $700k from Proactive and Predictive Information Assurance for Next Generation Systems (P2INGS) sponsored by the Advanced Research and Development Activity, a center for conducting information technology research. Cybenko will evaluate the applicability of Process Query Systems for the Cyber Indications and Warnings problem.

Dennis McGrath also received $400k as a sub-contract to General Dynamics Advanced Information Systems under the P2INGS program to research innovative techniques for early detection of cyber attacks.

In the Next Issue:
- Virtual Terrorism Response Academy
- PKI Bridge
- Sensor Networks