Counterintelligence Quarterly

July 2004

Issue 6

National Visual Analytics Center

The National Visual Analytics Center, established in 2004 by the Department of Homeland Security, will play a pivotal role in countering future terrorist attacks in the U.S. and around the globe.

The Center, led by Pacific Northwest National Laboratory (PNNL), will develop a national agenda to define the directions and priorities for future research and development (R&D) programs focused on visual analytics tools. A blue ribbon panel composed of leaders from academia, industry and government will set the national agenda on visual analytics.

Visual analytics tools, which are capable of creating images from complex multidimensional data, will enable analysts to effectively fuse and analyze the enormous, dynamic and complex information streams containing structured and unstructured text documents, measurements, images and video data. Analysts can use these high-impact, practical tools to more effectively identify signs of terrorist attacks in their earliest stages and ultimately thwart terrorist plots before they occur. *(Continued on page 3)*

Charles McQueary, Under Secretary for the Science & Technology Directorate of the Department of Homeland Security, announces that Pacific Northwest National Laboratory will lead the newly created National Visual Analytics Center. PNNL Director Len Peters joined him in making the announcement in mid-May.

A Leadership Message

William Magwood, Director, Office of Nuclear Energy, Science, and Technology

DOE's Nuclear Energy, Science and Technology (NE) program promotes secure, competitive and environmentally responsible nuclear technologies to serve the present and future energy needs of the United States and the world. With the significant energy and environmental challenges facing the nation in this new century, the benefits of clean and safe nuclear energy are increasingly apparent.

A key mission of DOE's nuclear energy research and development program is to strengthen that basic technology and, through some of the most advanced civilian technology research being conducted today, chart the way toward introduction of the next generation of nuclear power plants.

The Office of Nuclear Energy, Science and Technology also has responsibilities for space and defense nuclear power systems, advanced nuclear research and development, isotope production and distribution, nuclear facilities management, and nuclear fuel security.

In most of NE's activities, considerable effort has been made in cooperating with the international community. NE has a very wide range of international contacts in many countries and NE staff travel to many nations to pursue the offices broad nuclear technology agenda.

The briefing and debriefing program conducted by the Office of Counterintelligence provides essential support to NE's mission. This program is geared to maintaining interactions with NE travelers going to a select number of foreign countries as well as interacting with NE hosts of foreign visitors from specific countries. The information related by NE personnel is combined with information acquired by counterintelligence offices across the DOE complex.

Collectively, this information provides an overarching view of issues that are of counterintelligence concern that could be related to a specific DOE program, office, or laboratory. Thus, if there are concerns related to NE, I am advised of them by counterintelligence officials.

I encourage all DOE employees to realize that their interactions with the Office of Counterintelligence could result in the final piece of information that identifies a significant problem DOE officials must confront in order to protect the Department of Energy.

INSIDE THIS ISSUE

1 National Visual Analytics Center
1 Leadership Message
2 Action Against Foreign Lap Top Tampering
3 Prepare for Foreign Travel
4 Spies: Past and Present

TAKING ACTION AGAINST FOREIGN TRAVEL LAP TOP TAMPERING INCIDENTS

By Jenna McCarthy,
Office of Counterintelligence

Official foreign travel is utilized now more than ever to advance the Department of Energy's program objectives and mission. International interaction and cooperation contributes to many of our scientific breakthroughs and technological advances. However, this increased interaction also means greater risk of foreign intelligence collection activities. Lab scientists are prime targets for foreign intelligence services seeking to obtain sensitive information and proprietary knowledge.

In some instances, DOE/NNSA travelers can be targeted by foreign agents and lose sensitive/proprietary information and not even realize that they have been victimized. However, increasingly DOE/NNSA travelers have experienced or seen evidence of blatant targeting activities, and in response, are actively working to protect themselves and their colleagues against future attempts.

Dr. Joan B. Woodard, executive vice president of Sandia National Laboratories in Albuquerque, New Mexico recently shared an example of such vigilance, exemplified by one of her lab colleagues.

A Sandia colleague approached the local Office of Counterintelligence and shared his concern that gigabytes of sensitive data were leaked to foreign security services through improper handling of laptops on his visit to a sensitive foreign country. This individual (who has requested to remain unnamed) attended a counterintelligence pre-brief for his trip abroad and was made aware in advance of his trip that security police in this sensitive country could be expected to tamper with laptops.

This individual made his trip to this particular sensitive foreign country with a small DOE/NNSA lab delegation. As they arrived for the visit, security officials asked them to sign a notice saying that electronic devices were not allowed (and must be checked at the hotel). The delegation checked three laptops in the hotel safe -- with the foreign security officials keeping the key.

The individual received his laptop back upon leaving the facility, but the screw securing the hard drive immediately fell out. While there are benign interpretations, this is just what would happen if the security officials had removed the hard drive for data copying and reinstalled it carelessly. The individual reported this to Sandia counterintelligence upon return. Fortunately, this resulted in no data loss for the individual because he had prepared a "travel laptop" with a fresh operating system and only the files he intended to disclose to the sensitive foreign country representatives.

However, this led him to discretely ask other Tri-Labs visitors to this country if they were taking a laptop to this site and what protections were in place. He found that his colleagues had taken unprotected laptops (equivalent to Sandia Restricted Network laptops). Based on his small sample, he estimated that 50% of Tri-Labs visitors have laptops with sensitive (albeit unclassified) data. He reported that he suspected this would amount to up to five hard drives per week being made available to this foreign intelligence service.

The idea that "there are countries where the Government can legally copy hard drives is so strange that people do not know how to react," he said. "Instead, they shake their head, pack their laptop, and go anyway," he told Woodard.

He wanted to do something in response, so he took action.

"This individual recommended that Sandia officially endorse "travel laptops," recounts Woodard. "In addition, he agreed to share this story with others as a "champion" to raise awareness on this issue."

"Since my colleague brought this to our attention, concensus has been reached that we should change the Corporate Process Requirement's (CPR) to require that travelers to sensitive foreign countries use a laptop drawn from and returned to a centrally managed pool that can be inspected after each trip and which will never be connected to the Sandia network," said Woodard. "Our Chief Information Officer, Melissa Murphy, agreed to take the action on getting the CPR changed."

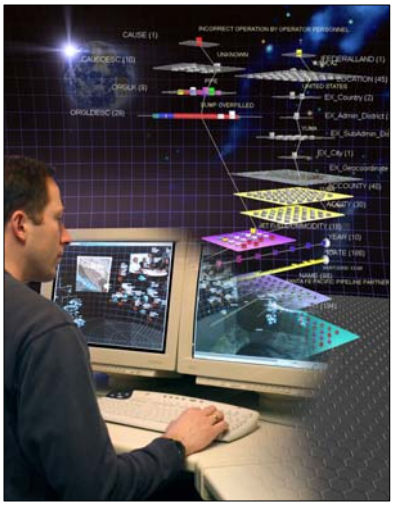
"This incident is a real example of what to many was only considered "a theoretical" concern," said Woodard. "One case at a time, we hope to have everyone achieve the right level of vigilance."

National Visual Analytics Center

(Continued from page 1)

The Center will provide the strategic direction, scientific leadership, education and coordination needed to discover, develop and implement innovative visual information analysis methods. In support of the Department of Homeland Security's missions, the Center will emphasize the following activities:

- R&D: conduct R&D in visual analytics technologies with an emphasis on proactive, predictive analysis to provide early warning of potential terrorist activities.
- Education: provide educational and hands-on opportunities for learning about the analytical environment to the next generation of scientists and engineers, and engage with university faculties in areas including curriculum development.
- Evaluation and implementation: establish test beds to evaluate new methods and support the adoption of new tools and methods in an



effort to speed the transfer of new technologies to analysts.

- Integration: coordinate R&D programs across funding agencies and research institutions to effectively execute the national R&D agenda for visual analytics.

PNNL is nationally and internationally recognized for scientific leadership and has a long history of high-impact contributions in information visualization and analysis for homeland security, intelligence and defense. The Center will capitalize on research conducted over the past 10 years by PNNL that has focused on providing innovative visual analytics tools to the intelligence community.

PNNL has extensive experience with the analytical challenges of the intelligence community. Its researchers have worked alongside analysts to bring fundamentally new analytical capabilities into their working environment. Interaction with analysts is critical not only to help them learn the mechanics of operating the new tools but also to help them adjust their analytical process to take maximum advantage of their new capabilities.

PNNL also has developed innovative tools such as the ARCH Model for Analysis and Information Discovery, an adaptive, flexible information acquisition and analysis method that couples human analysts with a knowledge management system in an interactive dialogue. The ARCH model provides

(Continued on page 4)

How to Prepare For Foreign Travel

So, what can you do to prepare for foreign travel? When traveling to sensitive foreign countries, all employees are required to complete a pre- and post-trip briefing. The specific actions that must be taken before and after traveling to sensitive foreign countries include:

- Schedule a pre-travel counterintelligence briefing with local Office of Counterintelligence offices before leaving.
- Participate in a debriefing with local counterintelligence officers (CIOs) upon your return from travel.

Pre-travel briefings are necessary because they provide the traveler the latest information concerning the threats posed in the foreign location. In addition they inform individuals how to guard against and what to expect when traveling to sensitive foreign countries. Also they educate DOE employees on specific methods that foreign intelligence services use to obtain information, which include:

- Elicitation – An effort in which seemingly normal conversation is contrived to extract information about individuals, their work, and their colleagues.
- Eavesdropping – Gathering information in social environments by listening in on a private conversation.
- Bag Operations – Efforts to steal, photograph, or photocopy documents, magnetic media, and laptop computers. This could occur in one's hotel room, in an airport, in a conference room, or in any other situation where the opportunity presents itself and materials are vulnerable.
- Electronic Interpretation – Use of devices to electronically monitor an individual's use of modern telecommunications, office, hotel, portable telephones, faxes and computers.
- Technical Eavesdropping – Use of audio and visual devices, usually concealed in hotel rooms, restaurants, offices, cars and airplanes.

The post-travel debriefings also allow the Office of Counterintelligence to learn from lab plant employee's experiences while on travel, and use that information to enhance the effectiveness of future pre-briefings. Together they are necessary and effective remedies to advance our national security interests as well as our individual safety and security.

THE PAST—JULIUS AND ETHYL ROSENBERG

Julius and Ethel [Greenglass] Rosenberg became the first American civilians executed for spying. The Rosenbergs were convicted under the Espionage Act of 1917 for "Conspiracy to Commit Espionage." Despite worldwide appeals for clemency, shortly after 8:00PM, on June 19, 1953, they were put to death in the electric chair. They left behind two young sons, Michael and Robert.

President Eisenhower twice denied executive clemency. Conviction was based mainly on the testimony of David and Ruth Greenglass, Ethel's brother and sister-in-law. The government had arrested David and charged him with spying for the Soviet Union during the development of the atomic bomb by making secret sketches and drawings when he worked at Los Alamos. David originally said he was recruited to get information by Julius Rosenberg; however, he recently admitted that he lied about some of his testimony.

THE PRESENT— SPECIALIST RYAN ANDERSON

The military conducted an Article 32 hearing on May 12, 2004, to determine if a National Guardsman should be court-martialed on charges that he tried to assist al-Qaida and join the organization so he could conduct terrorist attacks. Spc. Ryan G. Anderson, a Muslim convert and member of the Washington National Guard, was arrested in February 2004 and charged with four counts of attempting to provide information to the terrorist network. The information allegedly involved U.S. troop movements and tactics. A fifth count disclosed in the May 12 hearing alleged that Anderson told undercover military personnel: "I wish to desert from the US Army. I wish to defect from the United States. I wish to join al-Qa'ida, train its members and conduct terrorist attacks." At his arraignment on June 25, 2004, Anderson did not enter a plea or say whether he wanted to be tried by a jury or a judge. His court martial is set for August 16, 2004.

LOCAL COUNTERINTELLIGENCE OFFICE CONTACT INFORMATION

Contact us:

By Email:
^OCINWREGION
OCINWREGION@RL.GOV

By Telephone: 373-1865

Visit our website at:

http://www.hanford.gov/oci/index.cfm

ARTICLE SUBMISSIONS AND READER FEEDBACK WELCOME!

Counterintelligence Quarterly: Reporting on the nexus between quality science, technology and counterintelligence

Published by:
U.S. Department of Energy
Office of Counterintelligence and
Office of Defense Nuclear Counterintelligence
1000 Independence Avenue, SW
Washington, DC 20585

Managing Editor:
Jenna McCarthy
Phone (202) 586-4982
Fax (202) 586-0551
email: ci.quarterly@cn.doe.gov

National Visual Analytics Center

(Continued from page 3)

an ideal framework for a visual analytics environment because it supports the unique needs of the analyst from information acquisition through discovery and analysis.

Education and training are critical to preparing individuals to serve national needs in multiple agencies, roles and functions. The Center will concentrate on developing meaningful educational activities and providing hands-on experiences to students. Students will have the opportunity to learn about the analytical environment through simulated decision-making and the use of threat data scenarios. They also will have the opportunity to work directly with NVAC scientists as interns and in classroom and laboratory settings.

The NVAC is seeking collaborators for R&D projects and integrated demonstrations. The Center will operate through partnerships with national, regional and local governments, academia, national laboratories and industry. To achieve the goals of a sustained flow of advanced, high-impact technologies and talents, the national Center will establish and collaborate with regional visual analytics centers that will provide a regional focus and presence. Key areas of collaboration will include research technology development, curriculum development, training research faculty and staff, faculty and student exchanges, education, and test and evaluation. A call for regional centers will be announced in late 2004 or early 2005.

For more information, contact Jim Thomas, Director NVAC, PNNL at jim.thomas@pnl.gov.