

# Counterintelligence Quarterly

April 2004

Issue 5



## RAMiTS: POTENTIAL LIFE SAVER HERE AND ABROAD

By Ron Walli, Oak Ridge National Laboratory

Developed in 2001, Oak Ridge National Laboratory's RAMiTS point-and-shoot portable instrument to protect people and the environment by protecting and analyzing chemicals has undergone a number of refinements extending its capabilities.

The RAMiTS (RAMan Tunable Integrated Sensor) device can identify and quantify a wide variety of chemicals and biological samples in mere seconds. Unique as the first battery-operated portable device with tunable filters and performance comparable to that of laboratory-scale instruments, RAMiTS received an *R&D 100 Award* in 2003. Awarded by *R&D Magazine*, *R&D 100 Awards* are for the year's most technologically significant innovations.

"The RAMiTS answers a critical demand for a rapid, simple, compact and cost-effective device for screening chemical species and biological agents for homeland defense," said

Tuan Vo-Dinh, principal developer and a member of ORNL's Life Sciences Division.

Technically, RAMiTS uses Raman detection technology, employing a helium neon laser, acousto-optic tunable filters and a photo sensor to detect toxic chemicals, TNT, byproducts from explosives, drugs and hundreds of chemicals. The material can be in liquid or powder form. Another recent upgrade makes it easier to use in ambient light.

Raman detection technology illuminates a sample with a laser beam and measures the reflected light. The light shows the vibration energies unique to each compound in the sample, and a newly developed software interface identifies the substance. Prior to the development of acousto-optic tunable filters, the technology was impractical for field use.

An acousto-optic tunable filter is a solid-state optical bypass filter that can be tuned to various wavelengths. Because the filter is solid-state and has no moving parts, it is rugged and ideal for field application. Operation of the instrument is simple.

"We designed it to be used by people with no special skills," Vo-Dinh said. "The user merely points a probe at the substance to be tested and touches the start button on the touchscreen display. In 11 seconds, the instrument will tell the user what chemical or compound is present."

Vo-Dinh, who has won seven *R&D 100 Awards*, expects the instrument to be useful for environmental monitoring, medical diagnostics, health protection, food inspection, law en-

(Continued on page 2)

## A LEADERSHIP MESSAGE

Paul M. Longworth, Deputy Administrator for Defense Nuclear Nonproliferation



The mission of the National Nuclear Security Administration's (NNSA) Office of Defense Nuclear Nonproliferation (DNN) is to detect, prevent, and reverse nuclear proliferation, while mitigating the risks from nuclear operations. DNN accomplishes its mission by working closely with its international and regional partners as well as key federal agencies. The unique and invaluable expertise of the U.S. national laboratories further supports DNN mission activities.

DNN works with over 60 countries and international partners and allies to prevent and reduce nuclear proliferation and implement diverse programs that confront the complexities of the nuclear proliferation threat. We employ technology research and development, enhance nuclear safety, improve the security of nuclear and radiological materials worldwide, and support nonproliferation regimes and cooperation. We are eliminating the last vestiges of nuclear weapons-material production in Russia, blending down existing stocks of such material, and creating opportunities for Russia's nuclear experts to use their unique skills in peaceful, commercially viable ways.

To accomplish this mission, DNN programs collaborate closely with foreign counterparts, many from sensitive countries. While we rely on and look forward to successful international collaboration, we are mindful of the need to protect our sensitive or classified capabilities from compromise. We look to counterintelligence to provide support to DNN personnel, visits by the International Atomic Energy Agency, and other international protocols.

We appreciate the support counterintelligence provides us in accomplishing our nuclear nonproliferation mission.

## INSIDE THIS ISSUE

- 1 RAMiTS: Potential Life Saver Here and Abroad
- 1 Leadership Message
- 2 The Anonymous Web
- 3 The Internet and You
- 3 Customized CI Awareness Training

## RAMiTS: Potential Life Saver

### Here and Abroad

*(Continued from page 1)*

forcement and military applications.

"Instead of taking a sample and having to send it off to a laboratory, where it may take days to get results, this instrument enables people to get an instant analysis of samples in the field," Vo-Dinh said. "This will result in a great reduction not only in time, but also in cost."



intercept and read your messages, and discover who you're communicating with and what you are saying. The same is true with online chat rooms. If any of this information has been published to the Web, it will be accessible for a long, long time. It can be cached by web crawlers, such as Google, and displayed to Internet surfers long after the original page has been updated. In addition, other Webmasters may use content from your webpage, thereby propagating the information throughout the Web. The bottom line: Be very sure that the information you send out is information you do not mind sharing with the rest of the world.

### "War Driving" Wireless Networks

Hackers also engage in a tactic called "war driving." A hacker will drive around a neighborhood with a laptop, a wireless network card and a program that can find unprotected wireless access points (WAP) within a certain radius. Some war drivers use a larger antenna attached to their wireless card so they can increase the range from which they can find WAPs. This tactic can increase their range up to about six city blocks. Many war drivers will also use a Global Positioning System (GPS) connected to the serial port of the laptop so they can make a map of all of the unprotected WAPs in a given area. The war driver may publish that information to his or her friends and then all of them can surf the Net on your dime. The hacker may also enter new codes that allow them into your computer system and lock the rightful user out, or they may steal data or plant a Trojan virus.

## THE ANONYMOUS WEB

*By Chris Reynolds, Bechtel Nevada*

Home computers are clearly one of the top technological developments of the 20th century. A personal computer provides communication tools (email), informational tools (the Internet), educational tools (learning software and the Internet), entertainment (games and audio/video processing), and business management assistance (financial and word-processing software). Amazing tools most could not have imagined 20 years ago, are now, quite literally, at our finger tips. These every-day tools now help us collect and process information with record speed and efficiency and the Internet allows us to immediately share that information globally.

The downside to all of this? The potential loss of your privacy. However, despite the reality of these vulnerabilities, a few Internet-use protections and precautions can minimize your risk.

### Digital Footprints

When connecting to the Internet, your computer leaves behind a digital footprint called an *IP address*. Your IP address is recorded alongside the pages you accessed, the contents of your chat sessions, and email you thought was long gone. The Internet's 35,000 newsgroups are now fully archived and searchable. Combined with the tidbits of personal information you reveal while online: your name, address or employer, for instance, your com-

puter's IP address can be linked to your identity very quickly by those with a only minor computer savvy. Even if you provide false information to website registration forms, or use password-protected web services, your personal information can still easily be tracked down. Your IP address is linked to other sites you visit without falsifying information and the legitimate information will become clear to any marginally skilled identity thief.

Some computer-users utilize a Web Proxy Anonymizer to mask their real IP address from the Internet. While the Anonymizer is effective in hiding your information from the general Internet populace, Anonymizers track information about the people using their services. Criminals, terrorist organizations and foreign intelligence services could operate similar Anonymizer systems or co-opt them in some way to obtain true names of people using the service.

### Online Chat Rooms

Many people feel secure using online chat rooms simply because they are using an alias for a screen name. When your words scroll off the screen, it looks like they are gone forever, but that is not the case. Your IP address is recorded alongside your chat conversations, which are stored in company database logs. Also, Internet traffic, such as an email message, is similar to a postcard. Anyone with a little technical know-how can

What can you do about it? To protect your wireless devices and network, turn on your wired equivalent privacy (WEP) encryption systems that come standard with newer wireless computers or change the manufacturer's default settings on new computers. The WEP systems are basics for security. Also, you can set up an access control list so only pre-approved computers can access your network.

---

## THE INTERNET AND YOU: COUNTERINTELLIGENCE AWARENESS AND ELEC- TRONIC COMMUNICATION

Over the past several years, the emergence of Internet, Intranet and Extranet sites have been occurring at an impressive rate. Based on research performed by IBM, IDC and Forrester Research, the World Wide Web was expected to reach almost 500 million users by the end of 2003.

Given the power of the Internet, we

have to take special care to keep privileged information under wraps both at the office and at home. The Internet can be safe to use, however, individuals should be aware of the potential risks and special situations we, as a government contractor or employee, may face in using information technology and online tools. For cleared employees and contractors, access to sensitive information requires such individuals be responsible holders of that information at all times, both in and outside the workplace, in conversations in person and online.

What are the common mistakes that

people make while on the Internet? Mis-statements online occur much more frequently than deliberate counterintelligence or security breaches. In the workplace, counterintelligence and security guidelines are in place and the average employer/contractor is security conscious. But in the more relaxed setting of home, that same worker may be more likely to make casual and perhaps indiscreet conversation about a project or security clearance.

Following are some key questions

*(Continued on page 4)*

### CUSTOMIZED CI AWARENESS TRAINING OFFERED TO DOE/NNSA FACILITIES

*By Richard Skelton and Donald Fingleton, Ph.D., Counterintelligence Training Academy*

What might a scientist, an engineer, an engineering intern, a senior technologist from a national weapons laboratory, a nuclear courier (federal agent) from a field site, and several security and counterintelligence (CI) specialists have in common? They all recently met in a DOE classroom in Albuquerque, New Mexico for a series of new CI awareness courses, designed for all classifications of DOE/NNSA employees and contractors. Aside from the security and CI specialists in the group, most of the students did not even know that DOE/NNSA has a specialized academy delivering awareness training to DOE/NNSA headquarters and contractor sites -- free of charge to contractor labs and facilities across the DOE/NNSA Complex.

The Counterintelligence Training Academy (CITA) is an operating element of the DOE Office of Counterintelligence/NNSA Office of Defense Nuclear Counterintelligence (OCI/ODNCI). CITA is part of the Nonproliferation and National Security Institute (NNSI) located in Albuquerque. The courses reflect a continuing effort to enhance programs in response to requests from the OCI and ODNCI field counterintelligence officers. Two new courses are *Introduction to CI Awareness (CNA-103)*, a one-day seminar covering the foreign intelligence threat, the crime of espionage and the DOE reporting requirements; and *Terrorism Awareness: What You Need to Know (CNA-170)*, a two-hour seminar overview of the U.S. war on terrorism, DOE/NNSA's role in that war and individual awareness and response issues.

During the past year, CITA has also developed a "scientist-to-scientist" CI awareness program under the direction of Dr. Donald J. Fingleton, a CITA instructor, to reach out to and engage the scientific and engineering community. Dr. Fingleton — himself a DOE scientist with more than 30 years of lab experience — focuses on site-specific issues, ensuring they are relevant and customized for a given audience (e.g., material scientists, plasma physicists). Dr. Fingleton's topics are wide-ranging: research technology protection, intellectual property competition, open science and national security, weapons of mass destruction, and technology partnerships.

"CITA's goal is to be a value-added asset to the OCI/ODNCI, providing efficient, high impact, and cost-effective awareness training throughout the DOE/NNSA community," according to Senior Counterintelligence Officer and CITA Manager, Richard J. Sullivan.

The value of these 30-minute to two-hour presentations is evident in the number of CI referrals received from attendees identifying areas of concern. Results have been impressive. A presentation titled "Food and Agricultural Security" given at the Pacific Northwest National Laboratory (PNNL) generated positive media coverage and provided the impetus for a new PNNL initiative in this area. After a staffer of Senator Larry Craig (ID-R) attended a tailored version of the same presentation given at the Idaho National Engineering & Environmental Laboratory, the senator himself became interested in the subject.

For further information about arranging a CITA presentation at your site, contact your local Counterintelligence Officer.

(Continued from page 3)

and answers about security and counterintelligence awareness issues to consider when using electronic communication and other online tools.

**What should I do if I see inaccurate information about a sensitive topic on the Internet?** Nothing. Well-intentioned cleared individuals may see inaccurate information about a sensitive topic posted on the Internet, and their first impulse may be to contact the owner/author to correct this information. DO NOT. Your information and expertise in a classified area requires that you do not discuss classified information in any non-secure environment, following need-to-know guidelines. Even subtle nuances relating to classified subjects can be useful to skilled foreign intelligence agents, terrorist organizations and criminals.

**What are some of the dangers of identifying myself as a government employee or contractor while online?** If you are recognized as a government employee or contractor your words carry a weight that you may not intend. The common assumption is that you know more than you do or have access to classified information (which may or may not be the case). You may start to receive unwanted email solicitations and requests.

**What is "electronic spotting and assessing"?** Often the same techniques a foreign intelligence agent would use to approach you in a social setting while traveling abroad can be used on the Internet. The individual may try to strike up an online conversation, offer to do you a favor, and then ask for an innocuous favor in return. At this point, the message originator is trying to determine background information about you, your family and your job. If you respond, he/she may seek to break-off the electronic communication and seek a face-to-face meeting. These are warning signs. Should you encounter this type of potential

"spotting and assessing" you should contact your local Counterintelligence Officer immediately.

**What is the electronic "Good Samaritan" syndrome and how can I avoid falling victim to it?** Americans are helpful people. If Internet users in an electronic forum put out requests for information, they are likely to offer an immediate response. The problem comes in responding to a request for work-related technical information. The request may seem innocent – a student doing a paper on a given technology or specialty science. But how can you be sure the request is really coming from a student? You cannot. And, the response you send may reveal that you know much more than the average person about this subject. Employees and contractors should refrain from giving out technical information about their job function or field of expertise.

**How can I tell if someone is targeting me for sensitive information?** Any query or request for information on materials related to your job or your employer's proprietary information should be viewed with the utmost caution. (If in doubt as to what is proprietary, seek advice from your local counterintelligence officer. Typical query tactics include:

- ◆ Surveys offering a reward, gift or payment if completed.
- ◆ Instant message/email technical questions in an individual's area of expertise.
- ◆ Blatantly sending an email asking for sensitive information.

**When can online peer discussion/recognition be dangerous?** Many people may reveal information via the Internet with the goal of peer discussion, recognition or approval. But interested parties can combine random bits of information to produce a body of knowledge that is valuable to a foreign intelligence agency, a business competitor, a ter-

## 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

## LOCAL COUNTERINTELLIGENCE OFFICE CONTACT INFORMATION

By Email:

^OCINWREGION  
OCINWREGION@RL.GOV

By Telephone: 373-1865

Visit our website at:

[www.hanford.gov/oci/index.cfm](http://www.hanford.gov/oci/index.cfm)

rorist organization or criminals. The bottom line: do not share information you shouldn't. Remember also that for Q-cleared individuals, electronic contact with foreign nationals is reportable to your Counterintelligence Officer, just as you would report face-to-face contact. The Internet offers a variety of advantages to a foreign collector. They use the Internet to contact a wide variety of knowledgeable persons, with the intention to collect various pieces of information from each, based upon their area of expertise.