

Counterintelligence Quarterly

January 2004

Issue 4



HOMELAND SECURITY GETS HIGH-TECH HELP

By Dan Krotz, Lawrence Berkeley National Laboratory

A Lawrence Berkeley National Laboratory team has developed a portable device that uses neutrons to peer inside luggage and shipping containers to determine if explosive and fissile materials lurk inside.

The compact neutron source, developed by Ka-Ngo Leung and his colleagues in the Accelerator and Fusion Research Division, is ideal for both spot checks and continuous scanning of closed containers. The neutron yield of these generators is one thousand times greater than existing devices, and will allow the detection of smaller objects, faster screening, and more accurate discrimination among materials. "We use different energies of neutrons to penetrate different materials such as steel and aluminum," says Ka-Ngo Leung.

The tiny, tube-shaped neutron generator also represents a substantial improvement over commercial neutron generators, which are typically expensive and short-lived. At

a cost of roughly \$80,000, it is \$20,000 cheaper than generators of comparable capacity.

Neutron generators fire an ionized gas composed of hydrogen isotopes, either deuterium or tritium ions, at a metal target that also contains deuterium or tritium. The ions fuse with their counterparts in the target plate in a process that emits neutrons. These neutrons are then directed toward a structure that researchers want to examine - anything from brain tissue to crystals to luggage. The neutrons and gamma rays that bounce back are used to elucidate the internal makeup of the structure.

Unfortunately, today's compact generators have several drawbacks. Once the deuterium or tritium in the target plate is depleted, the generator no longer works. In addition, most neutron generators use an ion beam that is largely composed of two or three-atom molecules, which are less likely to produce neutrons in fusion reactions than single atoms. Perhaps most troublesome, today's portable neutron generators rely on deuterium-on-tritium reactions, which produce more neutrons than deuterium-on-deuterium reactions. However, any process that uses the unstable element tritium is burdened with layers of transport and safety concerns - not an ideal characteristic for a generator that may eventually be placed in airports and customs checkpoints.

Berkeley Lab's portable neutron generator tackles these problems head-on. First, the target plate no longer contains deuterium or tritium ions. Instead, a thin sheet of titanium and copper pitted with water-cooling channels is used. The deuterium or

A LEADERSHIP MESSAGE

Dr. Ray Orbach,
Director of the Office
of Science



World class science of the kind performed by the Office of Science laboratories, and of which we are so justifiably proud, is by necessity an international endeavor. Each year thousands of foreign scientists visit our facilities to collaborate, to run experiments, to share their insights, teach and learn. We in the DOE research community also must travel widely to ensure that our work is well-informed and at the forefront of discovery. However, with this practice comes a responsibility to understand the world we live in and take seriously threats to our national security. As Director of the Office of Science I want to take this opportunity to reiterate to all our valued scientists, contractors and employees the important work performed by our counterintelligence officers.

On numerous occasions related to my travels to sensitive countries, and/or in which I expect to discuss sensitive subjects or classified information, I have received counter intelligence debriefings that have been useful and very informative. These debriefings are consistent with Department of Energy Official Travel Order (DOE O 551.B), and are a vital part of the nation's counterintelligence effort. The DOE Office of Counterintelligence also conducts briefings and debriefings with the hosts of some categories of foreign visitors here in order to stay informed about how foreign visitors are traveling throughout the entire DOE laboratory system.

I encourage you to reach out to your local counterintelligence officers. Our continued partnership will build an increasingly more informed relationship between our two communities, and will help protect you as an individual, your laboratory, our Department, and our Nation's security.

INSIDE THIS ISSUE

- 1 Homeland Security Gets High-Tech Help
- 1 Leadership Message
- 2 Spies I Have Known
- 3 A Revolution in Espionage
- 3 Counterintelligence: A Team Effort

cont'd. on pg. 2

Homeland Security Gets High-Tech Help

cont'd. from pg. 1

tritium beam hits the target and continually adds new ions to the plate. This means the target cannot be depleted.

Second, the team increased the number of single atoms in the ion beam. Ninety percent of the ion beam is composed of single atoms, compared to 20 percent in beams produced by commercial generators.

"The beam is composed of single atoms instead of molecules. This emits more neutrons at the same energy," explains Jani Reijonen, also with the Accelerator and Fusion Research

Division.

Finally, the Berkeley neutron generator is engineered to rely on deuterium-on-deuterium reactions without decreasing the number of neutrons produced. The team accomplished this by using a cylindrical target instead of a two-dimensional plate. The rod-shaped ion source, which nests inside the cylinder, emits ions along its entire length. These ions strike the target that envelops it, a process that produces tens of trillions of neutrons per second.

"We can use deuterium reactions, which are much easier, cheaper, more

field-ready than reactions involving tritium," says Ka-Ngo Leung. "With these developments, we are striving to make the generator as efficient as possible."



Ka-Ngo Leung (right) and Jani Reijonen, both from the Accelerator and Fusion Research Division, stand beside the compact neutron generator.

SPIES I HAVE KNOWN: A PERSONAL ACCOUNT

By Al Romig, Sandia National Laboratory

We all recognize the name Klaus Fuchs, probably the most infamous spy to haunt Los Alamos during World War II. However, he was not alone. He had compatriots, including people like the Rosenbergs. But there was another key figure during this time period, known by government counterintelligence officers (FBI) as "Mlad." Mlad stole important information: the design of the explosive lens for the first implosion device.

For years, no one knew who he was. By the late 1960s/early 1970s, the FBI learned his identity but chose not to prosecute as it would mean making public classified information in any court proceedings. According to press reports, Mlad was a scientist living in England by the name of Ted Hall. He spent most of the last part of his career working in electron microscopy, a field shared by yours truly, in a former life.

In the 1970s and 1980s, both Ted and I worked in a very small field know as analytical electron microscopy. Ted and I had numerous opportunities to meet and discuss technical issues. For example in the early 1980s, Ted authored a chapter in a book I was working on as editor. And in 1986, a number of colleagues and I organized the annual electron microscopy conference in Albuquerque at which one of the sessions was named in Ted's honor, and for which he was the plenary speaker. During this conference, I was his host. He refers to this conference and his visit to the University of New Mexico campus, and Albuquerque as one that stirred up many memories for him related to his war time experiences. He also said that he did not return to Los Alamos during that summer of 1986 because his emotions "were simply too strong."

According to an article published in the *New York Times*

Magazine in 1997, the National Security Agency released a decrypted November 1944 cable naming "Teodor Kholm" as a volunteer Soviet informant.

In late 1997/early 1998, Hall gave a televised interview to the producers of CNN's "Cold War" documentary series in which he confirmed on camera, in very explicit language, his decision to give atomic information to the Soviet Union. Here is Hall's statement, as it appeared in March 1998 in Episode No. 21 of CNN's "Cold War" documentary: "I decided to give atomic secrets to the Russians because it seemed to me that it was important that there should be no monopoly, which could turn one nation into a menace and turn it loose on the world as ... as Nazi Germany developed. There seemed to be only one answer to what one should do. The right thing to do was to act to break the American monopoly."

In 1998 Hall also spoke to a BBC interview about his motivations: "Antagonists persist in the view that if I did something of this sort, it was to help the Soviet Union. It wasn't. Any action of that sort was, was, well, pardon the grandiose term, but I cannot think of another, was to help the world."

Hall's full story is covered in *Bombshell: The Secret Story of America's Unknown American Spy Conspiracy*, by Joseph Albright and Marcia Kunstel (Random House/Times Books, 1997).

Ted Hall died in November 1999 in Cambridge, England after a lengthy struggle with cancer and Parkinson Disease. For the latter half of his life he was viewed as no longer a threat, particularly once the Soviets developed their own nuclear weapon. According to these press reports, Hall was motivated by idealism, not nationalism, which is likely to be the case with a spy today. He felt the world would be more

cont'd. on pg. 3

Spies I Have Known

cont'd. from pg. 3

stable if there was not a nuclear monopoly. He feared that at the end of the war, a Depression-like era would return to the United States and we would slide into fascism, with horrible consequences if we were the only nuclear power. Once there was a nuclear balance, Ted's idealistic sentiments were realized and he returned to a scientific life totally unrelated to weapons and espionage.

Why do I tell this story, besides the fact that I like to tell it? If you had met Ted, you would have instantly thought he is simply a gentleman and a scientist. Even if you knew he worked on the Manhattan project, and he shared his stories with you, as he did with me (although never this one), you would never suspect him of being a spy.

Given our value of integrity here at Sandia, and throughout the DOE Complex, we would never assume that someone would steal information. We also know that these labs and plants are full of bright people, so we are not naturally vigilant against the accidental compromise of sensitive or classified information. We just don't expect smart people to make mistakes and due to our value of the individual we also don't like to look over each others' shoulders. Just as others and I never suspected Ted, we are likely never to suspect one of our co-workers or colleagues. But the fact remains that a primary issue we face, every day across government, throughout the DOE Complex, and within our own lab/plant environment, is the risk of the potential compromise of classified information.

So, what can be done about it? The answer is continued vigilance through counterintelligence training and awareness, and procedures to prevent mistakes and at the same time, make it difficult for anyone trying to intentionally compromise material.

By the way, I once met a scientist at Harvard who was Klaus Fuchs' roommate, who told me "You never would have suspected...."

Dr. Alton Romig is the Vice President for the NonProliferation and Assessments Program at Sandia National Laboratory.

A REVOLUTION IN ESPIONAGE

By Al Romig, Sandia National Laboratory

How could classified information potentially be compromised today? Through a variety of ways, of course, but there are mainly three methods:

- (a) a spy among us;
- (b) a remote surveillance attempt via computer hacking; or
- (c) an accident.

The likelihood of occurrence increases as we go down the list. It may be unlikely that we have a spy among us, but hacking incidents are on the increase and as humans, we all make mistakes. In the past, it may have taken "tons of paper" to steal or inadvertently lose track of significant amounts of classified information, the computer has made the possibility of major losses much easier via a zip drive or email. The ability to lose so much data, so quickly, has given rise to the term "revolution in espionage." However, in all three scenarios, there is a human element that is the focus for all detection and deterrence.

Contact your local counterintelligence officer to learn more about counterintelligence awareness and what you can do to protect your information and improve personal and workplace security.

COUNTERINTELLIGENCE: A TEAM EFFORT

By Darlene M. Holseth, Bechtel Nevada

Counterintelligence (CI) can mean many things, depending on your agency or environment. The DOE/NNSA defensive CI program is defined in Executive Order 12333: *Information gathered and activities conducted to detect and protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities, but not including personnel, physical, document or communications security programs.*

In labs and facilities across the DOE/NNSA complex, a CI team is directing this effort. Local CI programs are comprised of CI officers, analysts, cyber technical experts, administrative personnel, many of whom are retired special agents from various federal organizations such as the Federal Bureau of Investigation, the Central Intelligence Agency, the Air Force Office of Special Investigations and other federal agencies. A wealth of experience is available working together to achieve common goals to defend national security interests.

Counterintelligence officers (CIOs) serving in labs and plant facilities provide briefings and debriefings with various laboratory personnel: those who engage in travel to sensitive countries, and/or cover sensitive subjects or classified information during their trip. CIOs also conduct briefings and debriefings with the hosts of certain categories of foreign visitors/assignees. The briefing is to raise awareness of hosts/escorts on the potential for collection activities targeting DOE/NNSA interests. The debriefing process is used to obtain information of value to the DOE/NNSA defensive posture and the US Intelligence Community as a whole in identifying, mitigating and stopping collection efforts directed against the department and/or the United States. The information provided by DOE/NNSA personnel in these debriefs, and the assistance it provides in strengthening our national defense, is invaluable.

The DOE/NNSA investigations program is another function of the CIO. The

cont'd. on pg. 4

Counterintelligence: A Team Effort

cont'd. from pg. 3

advancement of national security and scientific interests is a high priority for the United States, now more so than ever. Given this critical responsibility, the integrity of our personnel is integral in the protection of our national assets. If a situation warrants an investigation, a formal process is conducted by the CIO and overseen by the Senior CIO. In rare cases, the CI Office will refer the investigation to the FBI if the findings meet the requirements outlined in *Section 811 of the Intelligence Authorization Act of 1995*.

The intent is to detect an insider betraying their country/company for their own advantage or to identify the collection activities of foreign entities. However, most investigations conducted to resolve unusual situations are usually nothing more than that: unusual situations. The investigations are done to determine the cause or details around unusual circumstances or inconsistencies to rule out intentional violations or espionage, thereby protecting all concerned: the individual, the company and national security.

The latest wave of collection activities directed against the United States is often cyber-related. Having identified this vulnerability, most DOE/NNSA CI offices now employ a CI cyber technical expert to address this threat. CI cyber technical experts are trained in the CI discipline and chartered to stay abreast of the ever-changing cyber world. Specifically, their focus is to gather information and conduct activities to protect against the cyber dimensions of espionage, other intelligence activities, or sabotage that target or threaten DOE/NNSA, its associated institutions, or the critical infrastructures of the U.S. Energy Sector. These CI personnel work closely with the DOE Office of the Chief Information Officer, the DOE Office of Independent Oversight, and the FBI's National Infrastructure Protection Center to execute their mission.

Counterintelligence analysts are dedicated to the more intricate

identification of potential collection activities targeting our personnel and resources. These highly trained individuals review data concerning collection efforts directed against DOE/NNSA employees and contractors here and abroad. They provide valuable information on the modus operandi of specific targeting directed against our facilities and the nation. This type of current information is often compiled in assessments, which are shared with DOE/NNSA contractor/employee groups.

Our administrative assistants, as with most offices, hold the office together. CI administrative personnel help to track personnel files, retrieve information and ensure a professional and courteous environment for employees and contractors as they meet with and request information from our CI team.

The most integral part of the CI team is the DOE/NNSA employee/contractor. Employee/contractor information regarding various targeting and elicitation attempts is vital to the CI program and its efforts to defend against, track and raise awareness of elicitation trends. Information such as the following should be reported:

- Unsolicited e-mail request from unknown, foreign sources;
- Unusual questions about job function, particularly while in a foreign environment;
- While in a foreign country, individuals that suspect they were being followed;
- Someone knew something about an individual that had not been divulged;
- At a conference/symposium, an employee/contractor is asked about a project completely unrelated to the topic of the conference/symposium
- Any professional, personal or financial relationship with a sensitive country foreign national.

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
1000 Independence Avenue, SW
Washington, DC 20585

Managing Editor:

Jenna McCarthy
Phone (202) 586-4982
Fax (202) 586-0551
email: ciquarterly@cn.doe.gov

LOCAL COUNTERINTELLIGENCE OFFICE CONTACT INFORMATION

Office of Counterintelligence
Richland Regional Office

Contact Us:

By Phone: 373-1865

By E-mail:
^OCINWREGION or
OCINWREGION@rl.gov

Local CIOs are chartered with providing employees/contractors with information to identify and mitigate these types of collection efforts. If employees/contractors do not report it, the CI team is limited in its ability to identify, defeat or mitigate such collection efforts.

Clearly, the most effective CI program is based on a knowledgeable and prepared workforce, working in partnership as a unified team. If you have any questions or would like further information about the DOE/NNSA CI program, please contact your local CI office.