



A Thermal Neutron Imaging System

Peter E. Vanier, Ph.D.
Brookhaven National Laboratory

Imagine that you are presented with a large number of sealed containers, and you are told that one or more might contain a nuclear explosive device of some sort. Your task is to find out which container contains the device, to localize its position within the container, and deduce its shape and size. Each target might be a steel drum or a truck-sized intermodal cargo container. The situation might be one of safeguarding our own nuclear inventory, or cooperative monitoring of a hypothetical dismantlement agreement, or protecting the borders from nuclear smuggling.

Currently, there are a number of passive techniques that can detect and analyze spontaneously emitted radiation as well as active techniques in which the container is irradiated and the transmitted data or reflected radiation is collected without actually opening it. Some techniques can provide a picture of the source material, showing the position and approximate size of the object within the container. However, the existing techniques have limitations in their ability to distinguish, within an acceptable amount of time, a threat from background radiation.

Brookhaven National Laboratory (BNL) has developed a new technique, called coded aperture thermal neutron imaging. Additional information acquired by this technique would provide the shape and location of materials containing a significant concentration of hydrogen surrounding a neutron source - such as explosives.

Imaging helps to identify man-made

"point" sources. In addition, the BNL coded aperture system is the only demonstrated technique that records the directions in which thermal neutrons are traveling. This information provides a unique detailed view of the source and its surroundings that complements the data available from other techniques. The BNL device is the first and only neutron camera of its kind. Since it can be scaled up to a square meter or more in size, it could provide the best means of detecting an improvised nuclear device at significant stand-off distances.



Fig. 1. Position-sensitive neutron detector

Fast neutrons emitted by spontaneous fission are efficiently slowed down by collisions with hydrogen until they reach thermal energy. Both the fast and the thermal neutrons can pass through significant thicknesses of metals including steel or lead, and can travel more than 60 meters through the air. A common way of detecting neutrons uses pressurized helium-3 gas tubes sensitive only to thermal neutrons. In order to detect the fast neutrons, these tubes are often embedded in blocks of polyethylene that slow down the neutrons before they enter the helium-3 gas tubes. Although this method is quite efficient in counting the total number of neutrons, it does not provide information on the direction from which each neutron came. To locate a source of neutrons with a traditional moderated helium-3 tube, one has to move the detector around in a systematic pattern and record the

INSIDE THIS ISSUE

- 1 A Thermal Neutron Imaging System
- 2 Cyber-Insider Awareness for System Administrators
- 3 Protecting Your Laptop
- 4 CI Press Highlights
- 4 Book Review

LETTER FROM THE CHIEF

By Catherine Sheppard

I am pleased to invite your attention to this third edition of the **Counterintelligence Quarterly** and encourage you to share it with colleagues. The NNSA Office of Defense Nuclear Counterintelligence and the DOE Office of Counterintelligence provide articles to develop an awareness of the counterintelligence and counterterrorism threats potentially faced by DOE/NNSA employees. Employee awareness is vital to our ability to counter the efforts of foreign intelligence services and foreign corporations who may be collecting DOE/NNSA classified or proprietary information. Report information or concerns to your local counterintelligence office. Together we can help ensure our individual security as well as the security of the Department of Energy and the Nation.

count rate repeatedly to determine gradients in the neutron density. This can be a tedious exercise, and does not provide information on the shape or

cont'd. on pg. 2

Thermal Neutron Imaging

cont'd. from pg. 1

size of the source or its exact location within a closed container.

The BNL thermal neutron camera is based on a helium-3 position-sensitive multi-wire proportional counter that determines the location of a neutron interaction to within 1 mm (see Fig. 1). Such detectors have been developed by BNL's Instrumentation Division for the study of protein crystal structure using collimated beams of low-energy neutrons. Recent improvements in the position-decoding electronics have replaced two rack-mounted crates of nuclear instrumentation modules with a single custom data acquisition board. This detector acts as the film of a box camera and we could use a simple

pinhole instead of a lens to create an image in which the source and the pinhole would be in alignment with a particular spot on the detector. However, most of the available neutrons would not pass through the pinhole, and the efficiency of the camera would be very low. Therefore, we use an arrangement of a large number of pinholes, known as a coded aperture (see Fig. 2), which casts a complex shadow on the detector. A computer program decodes the shadow and calculates the image of the source.

This system demonstrates the principles for locating sources of thermal neutrons by a stand-off technique, as well as visualizing the shapes of nearby sources. When combined with active interrogation, the

neutron camera could be used to provide an alternative means of contrast using backscattered neutrons or neutrons generated by photo-fission reactions.



Fig. 2. Coded aperture camera

Cyber-Insider Awareness for System Administrators

By William Von Elm, Office of Counterintelligence, Information and Special Technology Program

Traditionally, the term "insider threat" is associated with an individual who has valid access to classified information resources and the motivation (emotional, philosophical, economic, etc.) to either compromise those resources themselves or assist an outsider in compromising them. Indeed history is littered with the names of individuals like Fuchs, Walker, Howard, Ames, and Hanssen who have done just that.

In the cyber realm, however, the 'insiders' may not necessarily have the immediate access to highly classified information that a nuclear weapons designer like Klaus Fuchs, or a Navy code clerk like John Walker, or a CIA counterintelligence officer like Aldrich Ames would have. Likewise the actions of malicious 'cyber insiders' are rarely as dramatic as Ed Howard leaping from a moving car to elude FBI surveillance or as overt as Robert Hanssen stuffing garbage bags full of top secret documents under foot bridges in public parks. Because malicious cyber insiders enjoy the ease of communication and anonymity, their activities can be far more pedestrian and their pedigrees far more unremarkable than one might expect

The ultimate goal of any intelligence operation is the prosecution of some form of information warfare. The intelligence operative seeks information considered important by his adversary and the means to access, copy, transfer, or even modify it. In intelligence terms the 'important information' itself is referred to as 'primary intelligence' while information relating to the accessing, copying, transferring, and modifying of this primary intelligence is referred to as 'operational intelligence.' These considerations, from the point of view of a foreign

intelligence service or terrorist organization intent on conducting information warfare against the United States via an attack on the Department of Energy (DOE), would translate into:

- A search for primary intelligence.
- A search for operational intelligence to enable access to the primary intelligence.
- Attempts to use the resources discovered by the operational intelligence search to access either the primary intelligence or more operational intelligence and transfer it to the control of the foreign intelligence service or terrorist organization.

Therefore, in order to identify a potential malicious insider, system administrators need first to be able to identify possible sources of primary and operational intelligence on their networks.

Since system administrators are usually more closely attuned to the information infrastructure itself than to the information stored on it, they will likely be more familiar with the operational intelligence elements associated with their networks and systems than with the primary intelligence contained by them. There are important elements of operational intelligence that if known to a foreign intelligence service could be used to compromise network security and allow the primary intelligence to be lost. This would include information such as IP addresses of name servers, firewalls, authentication servers, VPN servers, and routers, as well as versions and patch levels of various

cont'd. on pg. 3

Cyber-Insider Awareness

cont'd. from pg. 2

operating systems and server software, various system and network account passwords, and the type and locations of intrusion detection systems deployed on the network. These are all part of everyday knowledge for the system administrator. Since these operational details are rarely advertised to the outside world, outsiders must usually resort to conspicuous and highly suspicious activities such as port/vulnerability scanning and brute force attacks in order to find and exploit them while many system administrators, in an attempt to promote a "user friendly" atmosphere, will politely provide much of the same information to any insider who takes the time to ask. This potential abuse of trust on the part of an insider is the single most important element of the "insider threat" to cyber information.

Perhaps the greatest fallacy indulged by network managers, administrators, and users is the belief that, because there is no classified information resident on their network, they have no counterintelligence concerns. While it is certainly true that the classified information held by DOE is some of the most aggressively sought after primary intelligence in the world, it is not by any means the only DOE information that is targeted by foreign intelligence services or terrorist organizations. Open source information on DOE research into "dual use" technologies such as lasers, particle physics, cryogenics, metallurgy, materials science, high performance computers, and bio-engineering can all be of use to nations or non-governmental entities seeking to establish or advance various weapons of mass destruction programs. Other "sensitive but unclassified" information on hazardous materials handling and storage, environmental hazards, and various types of unclassified nuclear information is of potential use to terrorist organizations. Information generated as part of Corporate Research and Development Agreements with industrial partners can be the subject of industrial

TRAVELING WITH A LAPTOP COMPUTER

By: Polly Leinius, Oak Ridge Office of Counterintelligence

According to FBI statistics, one out of every ten laptop computers will be stolen within the first 12 months of purchase, 90% of them will never be recovered and financial loss due to laptop theft has been second only to loss due to computer viruses for the last seven years running. Also, did you know ... In 2001, 591,000 laptop computers were reported stolen in the United States!

When a laptop is stolen, it is unknown whether it was taken for the value of the data or the value of the computer. Costly and inconvenient, the theft of a laptop computer is certainly significant, but when coupled with the potential loss of sensitive or proprietary government, commercial or scientific information, the loss could be much more devastating.

Laptops taken on travel outside of the United States are even more vulnerable to theft and unauthorized access. Airports and other venues of public transportation offer an inviting atmosphere for thieves due to large crowds, hectic schedules, and weary travelers. Laptop thefts commonly occur in places where people set them down – at security checkpoints, pay phones, lounges, restaurants, check-in lines, and restrooms. If possible, travelers should avoid taking a laptop on foreign travel; however, if absolutely necessary, remember the following tips:

En Route

- Keep your laptop with you at all times.
- A diversion or disturbance of some kind may be created for the purpose of appropriating your laptop.
- Transport your laptop in a bag that does not resemble a laptop carrying case.
- Do not place your laptop in checked baggage.
- Do not place your laptop on the airport's security conveyor belt until you are sure no one in front of you is being delayed.
- Do not store your laptop in an airport or train station locker.

Overseas

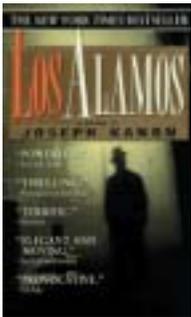
- Avoid connecting to any networked systems.
- Do not allow anyone else to use your laptop.
- Do not leave the laptop unattended – even for short periods of time.
- Do not load any software programs that are offered/provided by your foreign hosts.
- Be aware that foreign ISP's are usually monitored.
- Be alert to indications that your laptop may have been tampered with, for example: files missing or added; the battery seems unusually low; desktop has been rearranged; and/or screws are loose or missing.

If unique circumstances preclude you from being able to follow these guidelines, contact your local CI Office upon return. DO NOT connect the laptop to any DOE networks until after you have consulted with your local Computer Security team.

espionage and its loss or theft can lead to serious legal consequences for DOE and the U.S. government.

Finally, and most seriously, foreign intelligence services and terrorist organizations can use personal information, such as curricula vitae, employment files, and medical records, stored on the network to spot candidates who can either be recruited or coerced into providing whatever primary or operational intelligence that may be required. In addition to the

primary intelligence represented by all these sources, the cyber infrastructure of DOE itself is an attractive intelligence target since it offers large processing capacity coupled with the capability of storing (or hiding) and rapidly moving large amounts of data (or primary intelligence) gleaned from multiple sources. After all, the infrastructure was designed and built to facilitate research, which is the business of intelligence services as well as scientists.



Los Alamos, by Joseph Kanon

*Book Review by Janet
Goldman*

Los Alamos is an entertaining murder/mystery/spy novel that transports the reader back to the

days of the Manhattan Project at, of course, Los Alamos. Joseph Kanon's fictionalized account was published in 1997 and received rave reviews from a variety of sources. In Kanon's re-creation of the mysterious world of World War II Los Alamos, historical figures such as J. Robert Oppenheimer and General Leslie Groves are seamlessly woven into the plot along with fictional scientists who feverishly try to complete the "project" and with New Mexican locals who wonder about the secrecy of "the Hill."

When a Los Alamos security officer—himself a German refugee like many of the scientists—is found murdered in Santa Fe, U.S. Army Counterintelligence Officer Mike Connelly arrives to investigate the crime. He is tasked with finding the murderer while keeping his mission secret for the sake of the project. Even though someone eventually

confesses to the crime, Connelly is skeptical. After reviewing employees' personal history files and financial records, Connelly senses that the security officer could have been blackmailed and that a scientist's English wife—who spent unaccounted time alone in various European capitals before the war—might not be what she appears to be on the surface. Apparent diversions in the plot ultimately come together to confirm the worst; someone from the outside has infiltrated the Manhattan Project. And so, the intrigue of the counterintelligence officer in search of the spy begins.

The plot suspense is only partly responsible for the success of the book. For those familiar with the area, some of most enjoyable portions of the book describe the New Mexico landscape, particularly landmarks, roads, and the atmosphere surrounding Los Alamos, Santa Fe, and Chama. Despite tremendous changes in the past 50 years, today's northern New Mexico is clearly recognizable. This masterful rendition of time, place, and character during one of the most historical eras of modern time contributes immensely to the reader's enjoyment of the book.

Janet Goldman is an analyst with the U.S. Department of Energy Office of Counterintelligence in Washington, D.C.

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

RICHLAND REGIONAL OFFICE

Email:

^OCINWREGION
or
OCINWREGION@RL.GOV

Telephone: 373-1865

CI PRESS HIGHLIGHTS

Fermi Laboratory Assists DOE and Department of Justice in Arrest of Overseas Hacker

The U.S. Department of Energy Inspector General Gregory H. Friedman revealed that an IG investigation culminated in the search of a residence and arrest of a United Kingdom citizen in London, following an unprecedented joint investigation between the IG's Technology Crimes Section based in Washington, DC, and criminal investigators from New Scotland Yard.

Seventeen (17) unclassified U.S. Government computer systems were "hacked" at the Department's Fermi National Accelerator Laboratory in Batavia, Illinois. Compromised computers were then populated with copywrited software (known as "warez" in the hacker community). This made it possible for Internet users worldwide to access the compromised U.S. Government systems and download illegal copies of the software.

Initial forensic examinations of the Fermi computers conducted by the Office of Inspector General allowed investigators to identify the attacking overseas computer. New Scotland Yard, using this forensic information, tracked down and confirmed the owner of the computer in the United Kingdom. Additional forensic examination has begun on computers seized, and inquiries into all aspects of the attack continue. The seriousness of the alleged crime led the Office of Inspector General to send a Special Agent from its Technology Crimes Section to London to work directly with New Scotland Yard on this aspect of the case.

Friedman commended computer security personnel from the Fermi Laboratory who brought the intrusion to the attention of his office. He also expressed his appreciation for the effectiveness of the cooperative effort by the New Scotland Yard and his Technology Crimes Section.

(Source: Office of the Inspector General, United States Department of Energy, News Release, July 10, 2003)