LEGIBILITY NOTICE

A major purpose of the Technical Information Center is to provide the broadest dissemination possible of information contained in DOE's Research and Development Reports to business, industry, the academic community, and federal, state and local governments.

Although a small portion of this report is not reproducible, it is being made available to expedite the availability of information on the research discussed herein.

LA-UR -90-1956

LA-UR--90-1956

DE90 013185

TITLE THIEF - AN INTERACTIVE SIMULATION OF NUCLEAR MATERIALS SAFEGUARDS

AUTHOR(S) William D. Stanbro

SUBMITTED TO 31st Annual Meeting of the Institute of Nuclear Materials Management, Los Angeles, July 15-18, 1990

DISCLAIMER

Los Alamos

Los Alamos National Laboratory
Los Alamos, New Mexico 87545

MASTER

FORM NO. 836 R4
ST. NO. 2629 5/81

THIEF - AN INTERACTIVE SIMULATION OF NUCLEAR MATERIALS SAFEGUARDS*

William D. Stanbro
Safeguards Systems Group
Los Alamos National Laboratory
Los Alamos, New Mexico 87544

ABSTRACT

The safeguards community is facing an era in which it will be called upon to tighten protection of nuclear material. At the same time, it is probable that safeguards will face more competition for available resources from other activities such as environmental cleanup. To exist in this era, it will be necessary to understand and coordinate all aspects of the safeguards system. Because of the complexity of the interactions involved, this process puts a severe burden on designers and operators of safeguards systems. This paper presents a simulation tool developed at the Los Alamos National Laboratory to allow users to examine the interactions among safeguards elements as they apply to combating the insider threat. The tool consists of a microcomputer-based simulation in which the user takes the role of the insider trying to remove nuclear material from a facility. The safeguards system is run by the computer and consists of both physical protection and MC&A computer elements. All data elements describing a scenario can be altered by the user. The program can aid in training, as well as in developing threat scenarios.

INTRODUCTION

In many ways the most challenging scenarios for the diversion or theft of nuclear materials involve insiders. These individuals, whatever their motives, have legitimate access to at least parts of a facility, knowledge about facility operating practices, and adequate time to plan and execute their schemes. At the same time understanding potential vulnerabilities involving insiders is a complex task because of the subtleties of dealing with scenarios that so depend on comprehending the interactions of people. Unfortunately, the tools of operations research are very good at dealing with the behavior of machines and very bad at dealing with the behavior of human beings.

Gaming is a way of investigating the results of human interactions in conflict situations. It is a simulation that "employs human beings acting as themselves or playing roles in an environment that is either actual

*This work supported by the U.S. Department of Energy, Office of Safeguards and Security.

or simulated."[1] It is this interactive role of the human being that creates the possibility for enhanced insight into complex systems.

In this paper we will discuss a prototype interactive computer game called THIEF, which was developed by the Safeguards Systems Group at Los Alamos National Laboratory. This game is a tool to help safeguards professionals develop nonviolent, insider threat scenarios at their facilities. In THIEF the player takes the role of the insider trying to steal material from a facility. The computer plays the facility's safeguards system, including both physical protection and materials control and accounting elements.

A BRIEF HISTORY OF GAMING

The history of gaming is primarily the history of its use to understand and prepare for military conflict. While the origins of such strategy games as chess and Go are lost in antiquity, the adaptation of chess to understand war dates back at least to The King's Game of 1644.[2] A major advance came in 1811 when a Prussian lieutenant named von Reisswitz invented a war game played on maps rather than a square grid.[1] The game was further developed by von Reisswitz' son and named *Kriegsspiel*. This became a major tool of the Prussian and then German General Staffs through World War II. A primary use of these early games was training. However, in the late 19th century they rapidly became planning and research tools. Beginning with the Franco-Prussian war, most operations of the Prussian and German army were planned with the aid of war games. This was also true of the Japanese and United States Navies. Starting in the 1920s the U.S. Naval War College initiated a series of games to develop tactics for use against possible enemies. In the twenties the enemy was Britain, but in the thirties it became Japan. Admiral Chester Nimitz, in a speech at the U.S. Naval War College, credited the games played there with preparing the Navy for all of the tactics used by the Japanese in the Pacific War with the exception of the kamikaze attacks.[2]

Beginning with Prussian efforts to evaluate small arms performance in the Austro-Prussian War, games have been used to determine the effects of different weapon's parameters. One of the classic cases was

the use of games by the British Royal Navy to study the effect of an increase of 5 knots in the maximum speed of the planned Queen Elizabeth class battleships. The improvements in effectiveness indicated by this analysis were validated in both world wars.[1]

In the post-World War II period, the use of games to analyze conflict situations, including business and political battles as well as military ones, has exploded. A new feature is the availability of digital computers to expand the capabilities of the games. Computers have added a new dimension to gaming in that the computers can play a game and act as a labor saving tool or neutral controller. In order of increasing involvement, computer games range from exercises (such as a force-on-force exercise that involves human players on both sides) to analytic games, manual games, computer-assisted games, interactive computer games and games where the computer plays itself.[3]

A DESCRIPTION OF THIEF

THIEF is an interactive computer game in which the computer controls a nuclear facility's safeguards system, and the human player plays a nonviolent insider trying to remove nuclear material from the facility. The world of THIEF centers around a facility entered by the user. The facility is described by its fences, walls, doors, and gates. Inside the facility's buildings are the process equipment. The user provides the material flows and concentrations at points in the process lines.

The physical security system is represented by the facility structure and radiation, metal, and seismic detectors placed within the facility. The detector characteristics are specified by the user. The availability of human observation is also modeled. The materials accounting system is represented by a user-specified materials balance area (MBA) structure and user-specified analytical instrumentation. The materials accounting periods for each MBA are specified by the user. Based on the instruments' measurement variances and the material flows, the computer calculates inventory differences as well as the associated errors and determines if an alert should be called because of missing material. The computer also performs a trend analysis using Page's statistic to try to detect protracted diversion.

THIEF represents different classes of insiders by allowing the user to specify the information, location, and time accesses that the insider is allowed. The insider is allowed to perform any of a number of actions as he moves through the facility. These include picking up material or shielding, caching material within a facility, or attempting to remove material from a facility in a variety of ways.

THIEF is a continuous simulation, that is, the game steps through time at a constant rate. As time passes, the user commands the insider to perform the allowed set of actions. All of the insider actions are recorded to disk to provide a record of the actions taken.

IMPLEMENTING THIEF

THIEF was written in Turbo C and runs under MS-DOS on IBM-compatible microcomputers with 640 kilobytes of RAM. The program requires either EGA or VGA graphics. This requirement is based on the need for high resolution to support THIEF's graphical interface. In addition to the actual game, THIEF has a module to allow the users to input their own scenarios. An attempt has been made throughout the program to make it accessible to users with limited computer skills.

All data files are in ASCII format to allow easy checking outside the program. The records of the user's actions are in ASCII format and are readable with Lotus 1-2-3 or compatible spreadsheets to facilitate post-game analysis.

THE USE OF THIEF

We believe that THIEF will find uses in all of the traditional areas in which conflict simulation has been used, that is, training, planning, and research. The use of a common microcomputer platform and a user-friendly interface are based on a belief that the greatest benefit from the use of THIEF will be in allowing safeguards professionals to explore different scenarios in a relatively unstructured environment.

Looking back at Admiral Nimitz's speech to the Naval War College, two things are apparent. First is the great potential utility of games to prepare people for future contingencies. The second is that even after such a long and intensive series of games a significant tactic was missed by those involved. The use of kamikaze aircraft in the closing stages of the Pacific War resulted in the destruction of 34 Allied ships and damage to 368 others during the Okinawa campaign alone.[4] In many ways the kamikaze represented the forerunner of today's anti-ship cruise missiles such as the Exocets which destroyed the HMS Sheffield in the Falkland's War and almost sank the USS Stark in the Persian Gulf. The reason that this tactic was missed by the American Naval officers was that it was totally outside of their own culture. A similar danger exists in developing safeguards scenarios because the psychology of the potential thief is likely to be quite different from that of those involved in protecting nuclear materials. To the extent that tools such as THIEF allow easy investigation of diverse scenarios by different people, the greater will be the likelihood that important diversion paths will not be missed.

SUMMARY

THIEF is an interactive computer simulation game designed to help develop nonviolent, insider diversion and theft scenarios. Its implementation on a microcomputer and its user interface design are intended to encourage interaction between the users and their facility's safeguards system to increase the probability of discovering significant ways that nuclear material could be removed from a facility.

REFERENCES

1. G. D. Brewer and M. Shubik, *The War Game* (Harvard University Press, Cambridge, Massachusetts, 1979).

2. J. Prados. *Pentagon Games* (Harper and Row, New York, 1987).

3. T. B. Allen, *War Games* (McGraw-Hill, New York, 1987).

4. B. H. Liddell Hart, *History of the Second World War* (G. P. Putnum, New York, 1982).