A CASE STUDY OF HERESY IN PHYSICAL SECURITY

Earl R. Chapman

Lawrence Livermore National Laboratory: 7000 East Avenue, Livermore, CA 94550-9234 chapman6@llnl.gov

Sir Winston Churchill once spoke on the word "Empire," arguing that, regardless of the variety of connotations people may associate with the word, "Empire" is a perfectly polite, aptly descriptive and important concept. "Heresy" too is an aptly descriptive and important concept. (Heresy: "any belief or theory that is strongly at variance with established beliefs, customs, etc.").

Almost all facilities have at least one target of interest to its adversary. In the case of this audience, possible targets may be radiological materials or nuclear products. It is for the physical security specialist to assist the facility in developing a balanced, cost-effective system. But, too often physical security designs attempt to adhere to prescriptive rules for implementation without adjustment for the appropriateness of the prescribed elements. Those are the times for heresy or, if you prefer, to be strongly at variance with established custom. A reluctance to vary from the customary is understandable. Working on projects in Russia, I have experienced this reluctance many times as the final argument for or against some design element. But, I have also experienced successful feats of heresy. Let me share some of these examples with you.

I. INTRODUCTION

There is a debate quietly raging across the globe: Should Physical Security systems be based on prescriptive rules handed down from some level above the organizations that implement those systems? Should Physical Security systems be performance based, the specific means of attaining that performance determined at the level of the organizations that implement them? Or should there be some middle-ground designed to meet specific goals and address specific threats defined at a level above the implementing organization? In talking with people working with the International Atomic Energy Agency (IAEA), as it revises existing nuclear security documents and drafts new ones, I have sometimes participated in this debate and have come to understand that this question is just one of the issues the IAEA faces today. In this paper, I take my lead from Sir Winston Churchill and present a polite, aptly descriptive and important concept of heresy, ("any belief or theory that is strongly at variance with established beliefs, customs, etc.") in thinking about different perspectives on implementation of physical security requirements. Let me share with you some strong variance with established custom, using my experience working in Russia as a case study, in explanation of why I am a proponent of deviation from design elements and protective measures that can reasonably be modified.

II. WHAT HAS CHANGED IN RUSSIA?

A representative of one of Russia's premier nuclear weapons institutes (the Russian Federal Nuclear Center Zababakhin All-Russia Research Institute of Technical Physics) stated: "The physical security program at VNIITF was designed at a time when the former Soviet Union emphasized more strict control over individuals. Russia is now in a very different situation, where their diversification activities are resulting in an influx of business and industrial people whose reliability cannot be guaranteed through personnel screening. These changes in addition to the economic difficulties there have caused VNIITF to modify its security systems to apply to this different situation." [(1)] This observation says in a nutshell that the security blanket is gone. Even before September 11, 2001, Russia had begun to realize it must change its perspective and assumptions, not just of the world at large but of its own people as well. Russia had begun to realize that the time had come to depend more on reliable and sustainable technologies, than on the more fallible human component. But, that facet of the story is well known. I want to tell you something of what has molded their success, and of culture change.

Physical Security has been implemented with a very conservative focus by experts around the world. In many countries, there are federal-level codes and laws on protecting radiological and nuclear materials. Traditionally, those codes and laws typically prescribe the protection measures and system elements to be implemented, the devices to be used and the vendors who will supply them. Deviation might be severely punished. This type of regulatory requirements and implementation could lead to increased risks from:

1. **Unanticipated situations in the field:** For example, the code prescribes a buried

vibration cable along a perimeter fence line; but the fence borders on a road carrying heavy equipment and truck traffic generating needless nuisance alarms.

2. **Unintended consequences of regulations:** For example, by putting the prescribed grates on all windows of a building, you may pull the structure down with the added load.

3. **Unplanned applications of the regulations:** For example, installing hardened doors that have the prescribed certification stickers, even if you can demonstrate that the existing doors are sufficient for your implementation, needlessly increasing costs.

III. THREE TYPES OF DEVIATION

Typically, when Physical Security adheres to prescriptive rules documented in federal-level edicts, the system designer goes to the section of the manual pertaining to the particular target of interest, perhaps nuclear material or a radiological source. The designer reads the system elements and protective measures prescribed for an application, and then develops an implementation plan using those elements and measures — no less, no more. Without the ability to review the existing situation and consider the best implementation, the result may not be optimal. Russia has not yet developed and put into practice a formal process of deviation like that used in the U.S. Rather, many institutes in Russia may exercise the option to approve a deviation within their own organization, should they chose to accept that risk. In the U.S., we address the danger of blind adherence to prescriptive regulations with a formal process for authorized deviation and have implemented a formal process of variance, waiver, and exception. To that end, the Department of Energy (DOE) utilizes a process that formulates guidelines to deviate from prescribed regulations. Table I describes the three types of deviation that may be approved in the U.S. The table identifies the management level at which each type of deviation may be approved and the permissible duration of each type of deviation. The last column of the table gives examples I have witnessed of each type of deviation.

Table I. A Deviation Approval Process [(2)]

Deviation	Approval, as related to Special Nuclear Material (also, may be used for non-SNM issues)	Duration of Deviation	Examples
Variance: Approved conditions that technically vary from directive requirements, but afford equivalent levels of protection without compensatory measures.	In the US DOE arena, this is at the local site level. Allows for a faster approval process than the other two deviations.	No time limit, can be indefinite.	Russia: No dual-technology sensors are approved, so they use two sensors, each of a different technology than the other.
Waiver: Deviation from a directive that requires compensatory measures to preclude potential or real vulnerability.	Regional level, with high-level oversight concurrence.	Maximum of two years.	Russia: Rather than implement a full protection system, for a building used only occasionally, use additional guards when a target is present.
Exception: Deviation creating vulnerability for which there are no adequate compensatory measures.	Departmental/Secretarial level. Someone at a very high level must accept the particular risk identified.	Must be validated annually.	U.S.: A facility with Category 1 material is required to be surrounded by a barrier capable of stopping a vehicle of a specified weight, traveling at a specified rate of speed. This barrier may cost as much as $5M and not be in the budget for two years or more. The facility may choose to accept that risk until the barrier can be installed.

To provide a level of protection equal to that provided by following the Federal codes and regulations, use of either the Variance or Waiver type of deviation is preferable. The Variance type of deviation employs alternate but equal methods of protection, and is the most common type of deviation used in the U.S. because an alternate but equal method can usually be identified. The Waiver type of deviation employs compensatory measures and may be used instead. But, compensatory measures often equate to utilizing additional protective force personnel for the duration of the vulnerability, and hence may be more costly over time. The Exception type of deviation is seldom used, because it requires acceptance, of an identified risk, by the highest levels of the organization.

A Specific Russian Example of potential use of Deviation:

- **Problem:** A radioactive fuel storage facility that requires frequent Material Control & Accounting (MC&A) inventory of the storage ponds; but, high levels of radiation make frequent inventory checks unsafe or even life endangering.
- **Equivalent Measure:** Adding significant physical barriers could increase protection of the material, by significantly increasing adversary task delay time.
- **Solution Offered by a Variance:** Detailed analysis may show that a variance type deviation could allow a reduction in inventory frequency, by installing increased physical barriers and perhaps implementing a statistical sampling program.

It must be emphasized that the deviation process is not intended to be a tool of convenience; but rather, it is a means to comply with the intent of a regulation and provide an equally compliant level of protection, or provide risk acceptance.

IV. DEVIATION BEGINS WITH THE INDIVIDUAL, REGARDLESS OF STATE OR INDUSTRY – GUIDELINES TO CONSIDER.

Recognize the benefits of approaching solutions in a creative way, to the extent possible. One way you can do this is by recognizing those design elements and protective measures that perhaps should be deviated from, and when deviation is appropriate. It is generally appropriate and prudent to find alternative methods, of protecting a target of interest, when compliance with the guidelines could result in:

1. **Excessive costs:** For example, replacing hardened doors, even if they are evaluated in your vulnerability assessment to provide sufficient delay time, merely because those doors do not have the currently-prescribed certification stickers attached.
2. **Excessive time:** For example, made-to-order hardened doors can have a lead-time of as much as six months. Especially in a smaller project, such delays are not acceptable and only prolong the period of time the target is vulnerable, or that compensatory measures are needed.
3. **Serious safety issues:** For example, guard towers ten meters tall are prescribed, even though they are surrounded by trees thirty meters tall. The guards cannot see approaching aircraft. But, towers tall enough to see aircraft approaching may view only a limited area of ground below them. Also, their fields of fire are limited. So, while they may look good on paper, many professionals consider guard towers in a situation like this to be nothing more than intrusion detection sensors.
4. **Increased risks:** For example, life-safety codes may prescribe ladders be mounted, to the exterior of a multi-story building, beginning at a specified height. These ladders allow access to the roof by not only fire-fighting personnel, but by your adversary as well.

Begin a formal deviation by admitting to yourself that you are strongly at variance with the established custom — that design options are limited or nonexistent. Make a list of the design elements and protective measures you are strongly at variance with, why you are at variance with them and your thoughts on how deviation may resolve the problem. Discuss the nature of your concerns, your dilemma and your ideas, taking into account the risks in proposing a formal deviation. Next, discuss with your colleagues the proposed deviation:

1. What types of “regulatory deviations” are available, if any?
2. Would the proposed deviation be permanent or temporary?
3. Discuss with your colleagues the analysis and approval processes you propose to use.

4. Be certain to discuss any deviation policy, and means of coordination, with those who perform inspections and oversight.

Today, even though reluctance to make a formal deviation is evident in many places and for many reasons, there is increasing evidence that reluctance is decreasing in Russia. I see deviation becoming more a part of the Russian system. I see Russia becoming a stronger supporter of documenting the process, as it makes sense in a specific implementation; performance testing the process, to determine whether it really does make sense in that specific implementation and is performing as expected by the designers; adapting the process until it does perform as expected; and following the documented process for as long as doing so continues to make sense. When it no longer makes sense to follow a particular process, develop and document a new process that does make sense.

V. CONCLUSIONS

Ralph Waldo Emerson was speaking to us today as much as to anyone when he said: "A *foolish* consistency is the hobgoblin of small minds." It is for the Physical Security specialist to assist the facility in developing a balanced, cost-effective system. An important tool when developing any system is consideration of deviation from design elements and protective measures that can reasonably be modified.

REFERENCES

1. GENNADY TSYGANKOV, et al., "US/Russian Laboratory-to-Laboratory MPC&A Program at the VNIITF Institute, Chelyabinsk-70-May, 1996", *Non-Proliferation and Safeguards of Nuclear Materials in Russia*, Moscow, Russia, May 14-17, 1996
2. *DOE M 470.4-1 SAFEGUARDS AND SECURITY PROGRAM PLANNING AND MANAGEMENT*, pp. M-1 – M-7, (INITIATED BY: Office of Security and Safety Performance Assurance Approved: 8-26-05 Review: 8-26-07 Chg 1: 3-7-06)