Editor's Comments JPS Volume 2(1) (2007)·

Welcome to the second issue of *The Journal of Physical Security* (JPS). Just a few random thoughts and comments:

1. If you haven't already read John Mueller's book, Overblown: How Politicians and the Terrorism Industry Inflate National Security Threats, and Why We Believe Them", it is definitely worth a look. The author presents a provocative argument that our current homeland security response to terrorism is totally out of whack with the true threat, and is often misdirected and wasteful.

2. If you want to read something interesting, fun, and frightening simultaneously, check out these two books on drug counterfeiting: Katherine Eban, Dangerous Doses: How Counterfeiters Are Contaminating America's Drug Supply and Tim Phillips, Knockoff: The Deadly Trade in Counterfeit Goods: The True Story of the World's Fastest Growing Crime Wave. Counterfeiting (and tampering) with pharmaceuticals and other consumer products is going to be a huge issue in the coming years.

3. CSO ran an interesting article in August of 2006 entitled, *"Don't Shoot the Messenger: The first security assessment at my new employer wasn't supposed to be personal. It just ended up that way."* This is really about cyber security, but the issues discussed are probably even more relevant for physical security. See: http://www.csoonline.com/read/080106/col_undercover.html
By the way CSO (Chief Security Officer) Magazine continues to be one of the more thoughtful security trade journals, and often covers physical security concerns. Almost every issue has one or more articles that are quite fascinating. Plus it's free to qualified subscribers!

4. If you haven't perused the following web sites recently, they are definitely worth a look. While he's not focused on physical security *per se*, encryption and cyber-security guru Bruce Schneier always has interesting things going on at his web site (http://www.schneier.com/). (Bruce is on the JPS Editorial Board.) And Ross Anderson's home page at Cambridge University has a number of intriguing papers you can download that involve physical and electronic security issues (http://www.cl.cam.ac.uk/~rja14/).

5. In the Vulnerability Assessment Team at Los Alamos National Laboratory (http://pearl1.lanl.gov/external/c-adi/seals/index.shtml), we often work with a number of students ranging from high school students through graduate school. When we first interact with these students, many are very much at home with the idea of conducting research and development (R&D) on cyber security, but quite flabbergasted that there would be many unsolved R&D problems in physical security. What does this say about the future health of the field, and what can be done to change this perspective and attract more interest among young people, especially females and minorities?

6. As vulnerability assessors, we sometimes have a somewhat cynical view of security. This is both inevitable and useful. The following security maxims (or "rules of thumb") have arisen as a result of 15 years of work on physical security devices, systems, and programs. I would not claim they are absolute laws, but they probably do apply about 90% of the time.

Infinity Maxim: There are an unlimited number of security vulnerabilities, most of which will never be discovered (by the good guys or bad guys).

Arrogance Maxim: The ease of defeating a security device or system is proportional to how confident/arrogant the designer, manufacturer, or user is about it, and to how often they use words like "impossible" or "tamper-proof".

Ignorance is Bliss Maxim: The confidence that people have in security is inversely proportional to how much they know about it.

High-Tech Maxim: The amount of careful thinking that has gone into a given security device, system, or program is inversely proportional to the amount of high-technology it uses.

Schneier's Maxim: The more excited people are about a given security technology, the less they understand (1) that technology and (2) their own security problems.

Low-Tech Maxim: Low-tech attacks work (even against high-tech devices and systems).

Yipee Maxim: There are effective, simple, & low-cost countermeasures (at least partial countermeasures) to most security vulnerabilities.

Arg Maxim: But users, manufacturers, managers, and bureaucrats will be reluctant to implement them, often for reasons of inertia, bureaucracy, pride, fear, or wishful thinking.

Bob Knows a Guy Maxim: Most security products and services will be chosen by the end-user based on purchase price plus hype, rumor, innuendo, hearsay, and gossip.

I Just Work Here Maxim: No salesperson, engineer, or executive of a company that sells physical security products or services is prepared to answer a significant question about vulnerabilities, and few potential customers will ever ask them one.

Double Edge Sword Maxim: Within a few months of its availability, new technology helps the bad guys at least as much as it helps the good guys.

Familiarity Maxim: Any security technology becomes more vulnerable to attacks when it becomes more widely used, and when it has been used for a longer period of time.

Antique Maxim: A security device, system, or program is most vulnerable near the end of its life.

Payoff Maxim: The more money that can be made from defeating a technology, the more attacks, attackers, and hackers will appear.

I Hate You Maxim 1: The more a given technology is despised or distrusted, the more attacks, attackers, and hackers will appear.

I Hate You Maxim 2: The more a given technology causes hassles or annoys security personnel, the less effective it will be.

Shannon's (Kerckhoffs') Maxim: The adversaries know and understand the security hardware and strategies being employed.

Corollary to Shannon's Maxim: Thus, "Security by Obscurity", i.e. security based on keeping long-term secrets, is not a good idea.

Gossip Maxim: People and organizations can't keep secrets.

Rohrbach's Maxim: No security device, system, or program will ever be used properly (the way it was designed) all the time.

Rohrbach Was An Optimist Maxim: Few security devices, systems, or programs will ever be used properly.

Insider Risk Maxim: Most organizations will ignored or seriously underestimate the threat from insiders.

Father Knows Best Maxim: The amount that (non-security) senior managers in any organization know about security is inversely proportional to (1) how easy they think security is, and (2) how much they will micro-manage security and invent arbitrary rules.

Huh Maxim: When a (non-security) senior manager, bureaucrat, or government official talks publicly about security, he or she will almost always say something stupid and/or naïve.

Troublemaker Maxim: The probability that a security professional has been marginalized by his or her organization is proportional to his/her skill, creativity, knowledge, competence, and eagerness to provide effective security.

Throw the Bums Out Maxim: An organization that fires high-level security managers when there is a major security incident, or severely disciplines or fires low-level security personnel when there is a minor incident, will never have good security.

7. The *Journal of Physical Security* is primarily meant as a peer-reviewed, scholarly journal for theories, models, commentary, and research and development in the area of physical security. From time to time, however, we will have articles that are not peer-reviewed. This many include reprinted papers that have appeared elsewhere, reviews or viewpoint papers, essays, interviews, and my own editor's comments. You can assume, however, that any research paper that appears in JPS has been reviewed by at least two anonymous, independent reviewers, unless noted otherwise on the first page of the paper in question.

This issue also contains some non-peer-reviewed research papers (papers 2-5) that have come out of my own Los Alamos Vulnerability Assessment Team, and are marked as such. One of the reasons for founding JPS was our frustration at the absence of scholarly, peer-reviewed journals devoted to physical security. Finding a home for these papers elsewhere would probably be a challenge. We could, I suppose, devise some kind of anonymous peer-review process involving the Editorial Board but not the Editors that might resolve some of the conflict of interest in having the Vulnerability Assessment Team (which hosts JPS) publish papers in its own journal, but that is probably not worth the effort. If you find our non-peer reviewed papers just too much vanity self-publishing, feel free to ignore them.

8. As always, comments, suggestions, and complaints are welcome on any topic relevant to JPS. And please consider submitting a manuscript!

9. Thanks for your readership!

10. As always, the views expressed by the editor and authors in JPS are their own and should not necessarily be ascribed to Los Alamos National Laboratory, the United States Department of Energy, or the United States Government.

--Roger Johnston

· Full disclosure: The editor has no financial or other interests in any of the sources or references recommended here. He is, however, grateful to CSO for publishing an interview with him (http://www.csoonline.com/read/060107/fea_qa.html), in addition to placing a version of his (only partially serious) security self-assessment tool on the Internet (http://www2.csoonline.com/quizzes/security_assessment/index.php). He was not compensated for either.

Research Paper

Perceptions and the social-political aspects of nuclear power and nuclear waste disposal.

James David Ballard

California State University Northridge
Department of Sociology
18111 Nordhoff Street
Northridge, California 91330
United States of America

Introduction

The problems that many nuclear engineers, energy policy makers, industry officials, and risk regulators face when discussing the social and political aspects of their field can be summarized by one word: perception. The public perception of the dangers inherit in the portions of the fuel cycle associated with nuclear power generation and radioactive waste transportation and disposal is vastly different from the perceptions held by those within the nuclear infrastructure (i.e., policy makers, planners, designers, etc.).[i] These perceptual differentials hold the key to any discussion on the social and political aspects of nuclear related activities since they represent the very real, in their consequences, fears that the public has with respect to the industry and especially its related production inputs like nuclear materials and outputs like spent nuclear fuel (SNF).[ii]

This article will examine these perceptions and their effects in an effort to offer an atypical perspective, at least from the standard industry viewpoint, on the activities commonly associated with the nuclear power generation infrastructure. To accomplish this goal, the discussion will focus on three interrelated arguments. First, public perceptions have an influence on the ability of the nuclear energy infrastructure to operate within contemporary industrial societies. Secondly, events like those that transpired at the Three Mile Island nuclear power generation facility, the tragedies resulting from the failures of technology and the poor oversight by human caretakers at the Chernobyl site, and even seemingly unrelated events like the terrorist attacks on September 11, 2001, all have the potential to galvanize public perceptions against the nuclear industry and may increase the regulatory and social/political pressures on said infrastructure. Lastly, these same perceptions can exhibit themselves in many ways and could help to unite the various political action groups typically found in a given society and against the nuclear industry.

The conclusion of this essay will address some of the negative aspects of the nuclear infrastructure's resistance to, or in some cases the denial of the legitimacy of, such perceptions and how an understanding of the very real consequences of said perceptions can provide the industry with insights into their social, political and caretaker roles in contemporary society. The object of this argument is to highlight some of the various pressures that face those within the nuclear infrastructure and in the process help illustrate the latent effects of the typical "stonewall" attitude used by industry insiders when faced by the reality of criticisms based on non-technical based perceptions by non-industry social actors.[iii]

Public perceptions have influence

While many nuclear industry insiders believe that probabilities and their associate risk calculations have real meaning to the public, the fact remains that these calculations are not what drives the public's view of nuclear power and highly radioactive wastes. One suggestion to overcome the problem that can arise when the general public reacts badly to nuclear power and radioactive wastes is to: 1) conduct an analysis of the perceptions the public has on nuclear related issues and 2) to address their concerns in a non-confrontational and respectful manner.[iv] Prior to this being accomplished, it is necessary to understand how the differentials in industry and public perceptions come about and what effects they have on social and political debates surrounding the energy industry. As such this argument will attempt to highlight these issues in a manner that will allow for such understanding.

The social and political consequences of a perceptual differential between the industry and the public can be profound. Just think about the typically response of the nuclear industry to criticisms from outside, what can be termed social or political criticism. For a moment consider the hypothetical situation where the industry, or one of its representatives, contends that the risks of a nuclear power plant have already been studied and for the most part found to be meaningless, in terms of the probability or consequences. This industry reality is in direct opposition to the reality felt by the general public who quickly come to distrust these industry proclamations and find value in the perceptions of alternative experts who use their training in engineering, or risk modeling, to contend that the energy industry is using self serving calculations as the basis of their claims. The tension between these two positions is evident and while it

may be easy for the energy industry to dismiss the very real public fears that result, they should not be discarded so easily.[v]

A more tangible example of the perceptual divide represented herein can be found in the debates on the Yucca Mountain project in America. Recently one industry official testified in the American Congress regarding the chorus of social and political voices opposing the pending program to transport radioactive materials to the proposed Yucca geologic repository.[vi] Paraphrasing this testimony, this industry representative referred to the critical voices as a "cottage industry" intent on playing off of the irrational fears of the public and opposing progress by the industry.[vii]

The oppositional dialogue represented by such a comment, a distinct "we" verses "them" mentality, easily develops when perceptual differences are so profoundly disjointed. This real world example is not an atypical response when nuclear energy infrastructure proponents face intense questioning of their actions by the public, politicians, non-technical opposition forces, and/or even those within the industry who question choices made by the infrastructure managers regarding safety, security, and transportation.

Typically those who work within the energy infrastructure feel that such animosity towards social and political criticism is their only response given the emotionality, or even what they may term irrationality, of the opposition. Thus, such responses by the industry are seen by those within this infrastructure as self-protective and their proclamation is almost demanded given the antagonist claims and arguments of opponents.

Another way of seeing this is that such an industry response is not productive to the health and welfare of the industry and its workers; it will inevitably foster increased criticism by the opposition and can even engender amplified regulatory oversight since the public and non-sympathetic regulators and government officials see this attitude as a prime example of industrial arrogance. It is possible that such forms of corporate arrogance will just add fuel to the firestorm of public debates. They also show a clear disjunction between the perceptions expressed by the nuclear industry and those held by the public.

What may be difficult for many in the industry to comprehend, and perhaps this lack of understanding is one motive for these types of self-destructive attacks against social and political critics of the nuclear infrastructure, is that perceptions are socially and politically relative. They are *not and never will be* reducible to scientifically derived probabilities and typically industry risk assessment methodologies. Such profound perceptional differences as these can not be overcome by these forms of instrumental logic alone, they must be understood as to their point of origin, as to why they persist in the face of what the energy infrastructure considers valid evidence, and most importantly, a process must be engaged wherein the criticisms can be addressed by dialogue, not hostility.

In social scientific terms, the social construction of reality the social and political opponents of the energy industry engage in is a very powerful process. This construction of reality is a social process based on an internalized assessment of how people interact on the basis of symbols and signs. Such symbolic interactions help people assign meaning to their everyday experiences and perceptions. They shape how we view the

world and everything within that world, even those things we fear and dread, like radioactivity. Thus our life world, the everyday social world we inhabit, includes the social and political routines, rituals, and experiences that shape how we see the world and how we as social beings react to threats like those posed by nuclear power and radioactivity.[viii]

For many in the body politic, radioactivity is a part of the life world where they do not wish to delve. The have been socialized to believe that nuclear power is equated to nuclear war and the outcomes of a nuclear power plant (NPP) accident, or terrorist attack on a spent fuel pool or radioactive waste shipment, would be equated to the attacks on Hiroshima or Nagasaki.[ix] The bottom line is that due to such characterizations from popular culture and the internalization of such a normative structure, they seek out and value an alternative scientific literature. Due to these factors the public has horrific images attached to nuclear power. These images are difficult to mitigate by typical industry logic alone, or even worse by an industry insistence on using such seemingly normalized engineering presentations of risk calculations replete with references to 10^{-8} probabilities.[x]

This social reality is in direct opposition to those within the nuclear infrastructure and their everyday world of handling radioactive materials. To these industry insiders, the normalized rituals of their everyday experience and their intimate working knowledge of the materials and safety procedures therein, make any outside criticism seem less than creditable, especially if the critics use the public dialog of imminent annihilation that could become attached to nuclear power during an accident or hazardous incident.

To summarize what is a perceptual disjunction, to the general public, the common and everyday yellow placards and safety equipment used to protect health and safety in nuclear facilities are signs fraught with a vastly different symbolic meaning than those held within the energy infrastructure. The common everyday meanings associated with nuclear power escape those within the industry, at least with respect to risk perceptions, because of this perceptual disjunction.[xi]

While the non-industry perceptions may have been learned from movies and other non-technical sources, they hold a valued place in the everyday social and political culture of advanced technological societies. What is critical to understand is that the perceptual disjunction is very real in there consequences for the energy industry. Clearly, the disjunction between industry and public perceptions may be the result of differentials in education, training, risk knowledge, everyday experiences, and/or perceived "troubling" history publicly associated with all things nuclear.

Clearly, for those within the nuclear industry the world of working with radioactivity is very different than what the public feels about these materials. The industry insider typically sees risk, but not what is considered overt danger. The public sees risk and considers it a fatal danger just waiting to happen. Therein lays the rub, one perspective that sees all things nuclear as a tool of progress and social success and one that sees all things nuclear as a threat to health, safety, and security.

This type of perceptual disjunction may well be the origin of the social and political problems faced by the energy industry as an entity. When certain events transpire in the course of social life, these events galvanize public opinion and focus scrutiny on the normalized activities that transpire in the nuclear infrastructure. The next

section of this essay will examine these social pressures in an effort to show how perceptual differences can impact society and the nuclear power industry.

Galvanizing events

Advanced technologies have drawn opposition from social and political groups in the modern era, perhaps none more readily than nuclear power plants (NPP).[xii] The relatively few instances of serious problems with NPP and the potential for tragic consequences that may result from a failure of controls and/or that may be the result of outside forces are legitimate social and political concerns expressed by a variety of groups and movements in many places around the globe.[xiii]

The perceptions within the energy industry that such instances are either isolated problems or unrelated to the operations of most NPP also represent a similar dimension of the perceptual dialectic the industry has from public perceptions. This dichotomy is hard for energy insiders to grasp and as such makes it difficult to understand why the public has such fear and dread of normal everyday operations of NPP's. A quick review of three significant galvanizing events may help situate the link between such common public fears and the nuclear infrastructure.

The events surrounding the failure of controls at the Three Mile Island (TMI) nuclear power facility have had a powerful influence on the public and have had a significant impact on how the general public sees nuclear power generation.[xiv] On March 28, 1979, Unit 2 at TMI was beset by an incident that ended as the most serious commercial power plant operation accident in United States history. Adding to the problems this accident burdened the industry with was the fact that at the exact same time this accident transpired, the movie the *Chain Syndrome* was in theaters. The social and

political fusion of fact and fiction was instantaneous and the result is difficult for the public and energy industry to untwine, even 20 plus years *ex-post-facto*.

The intertwining of these two events was fortuitous for the moviemakers whose product popularity was more than enhanced as a result. What is important is that the images from this movie have had a significant impact on how the public views nuclear power in the post-TMI era. To illustrate, the perceived reality held by the public is not easily moderated when decades after the actual accident at TMI, the Nuclear Regulator Commission (NRC) notes that the "causes of the accident continue to be debated to this day ... (relevant) factors appear to have been a combination of personnel error, design deficiencies, and component failures" (NRC 2002).

After over twenty years of study, this regulatory body clearly states that no clear-cut answers are available as to why this accident transpired. The systematic failure of the human, regulatory, and technological controls in this particular instance are illustrative of why a profound distrust exists between the public and the nuclear infrastructure. As part of their function in society, regulatory bodies like the NRC must assure the public that such accidents are rare and that they are not worth the continuing fear of the body politic. Such claims are common when regulatory agencies are advocating for nuclear technologies to be used and/or expanded, yet this particular accident did transpire and the public somehow remembers the same agency and its pre-incident claims of low probability and downplayed fears of the consequences of such accidents. Such instances of perceptual disjunctions hold the potential to transform the debates on nuclear power and failure to recognize such a perceptual perspective is one factor in the divide between the industry and the public.

Similarly, the Soviet nuclear industry accident on April 26, 1986 at the Chernobyl power plant site is generally characterized as the worst accident in the history of nuclear energy. Similar to TMI, the social and political results of this event are difficult to overcome by probabilistic logic and again point out the disjunction between perceptions held by the public and those articulated within the industry.

While immediate fatalities at Chernobyl were relatively low (31 deaths), the worldwide body public was exposed to other facts: the need to establish a central contamination zone surrounding the damaged plant (~ 30 km); the results of a massive transfer of local residents with perhaps 100,000 permanently dislocated; details on the enrollment of hundreds of thousands into a medical registration system to track the health effects of this exposure; and particulars on the many other post-incident remediation efforts reported on by the world press.[xv] These developments present a symbolic picture that is difficult to purge from the public memory and equally arduous to overcome when discussing the role of NPP in contemporary society. One result faced by many industry insiders, despite their proclamations that this was an anomaly, is that the "benefits" of nuclear energy are ever increasingly more difficult to advocate when the results of an accident at an NPP are so evident, so dramatic, and potentially so socially and politically devastating.

The third galvanizing event discussed herein was the tragic events of September 11, 2001. The details are startling: terrorists used large commercial airliners to attack a highly symbolic target, the coordinated and suicidal efforts of a large group of attackers were successful, and the profound socio-economic effects evident in the aftermath were

socially and politically significant. These are troubling facts when one considers the fate of NPP.

In the aftermath of September 11, 2001, the possibility of similar attacks on NPP and/or the nefarious use of waste products (in transit or in spent fuel pools) as the source material for a radiological dispersal event have unfortunately become much more of a commonly held form of tactical knowledge. Couple this knowledge with the subsequent revelations that terrorist groups were already, and still are, considering the use of radiological dispersion devices and it is easier to see how such potentialities have dominated the popular media in the last several years and how such images came to be associated with nuclear power generation and the energy industry.[xvi]

The tactical progression of some violent groups towards strategies that threaten nuclear facilities and the energy industry, have started to reveal a deeply entrenched social and political reality behind the public's fearful perceptions of all things radioactive. Given the accidents noted above and the as yet to be known aftermaths of these same instances, what would happen if a large dedicated suicidal group of fanatics tried and succeeded in an attack against an NPP, or the SNF storage pools therein, and/or were successful in attacking a shipment of highly radioactive waste destined for a reprocessing plant and/or geologic storage facility? The questions reveals an uncertainly quotient that is part of the everyday operation of a nuclear facility, an unknown risk factor that is highlighted by such events.

The social distance the public feels from such risks is lessened during such galvanizing events, perhaps to a point of intolerance for the nuclear industry, but not always to this point of no return. So why are such fears important to understand?

Perhaps most importantly, they have the potential to act as a catalyst to action against nuclear power and the energy infrastructure. The next section of this essay will examine this opposition coalesce potential.

Uniting factors

The perceptual differences between the energy industry and the public are highlighted at those times when the public and politicians focus intensely on the safety of nuclear power or the various parts of fuel cycle that are related to energy production. Galvanizing events like those noted above are just the lens that helps to focus unwanted attention on the industry, but they will persist in the future. The reactions of the industry to criticisms resulting from such events are equally as sure to persist in the future. Both the reactions to galvanizing events by the public and the response to criticisms by energy insiders during times of crisis are evidence of the perceptual divide between the public and the energy infrastructure.[xvii]

This divide may be the most predictive aspect of the social and political barriers that are faced by the energy industry. These represent disconnect moments between the energy industry and the public and they are indicative of what can be termed bureaucratic anomie, a term used to describe how out of touch formal organizations can become with the reality commonly experienced by the pubic. The debates that transpire at these times show how the nuclear industry reify their own risk modeling and internalize a unshakable belief in their engineering prowess, while forgetting that the vast majority of the citizens do not understand their calculations and in fact mistrust their proclamations of low probability events, sufficient safety, and adequate security.

Thus, the social and political factors that result from such perceptual fracturing can produce significant resistance to nuclear power and the energy infrastructure behind its production. The technology that seems so trustworthy to industry insiders is not seen as reasonable or viable in light of such risks. The regulatory processes that oversee the nuclear industries everyday operations, generally without significant incidences, are quickly subject to being questioned because they cannot be trusted to assure absolute safety and freedom from problems during NPP operations.

The government and regulatory oversight of the energy infrastructure is almost instantly examined to insure that special energy industry interests are not given priority over public safety, and to insure that such bodies place a higher value on protection on human health and life than on industrial production. In short, the public recalculates the economics of the industry and the role of regulatory bodies during such times.

Thus, factors associated with the technology, regulation, oversight, and risk modeling come into question. The public distrust for sophisticated science is heightened and the standards of scientific proof that will be necessary for future projects will most likely be raised. The types of resistance factors noted above are further strengthened when industry representatives relegate the risks to the realm of impossible and demote public fears to characterizations of the opponents as ill-informed, delusional, and as the ranting of radicals and environmental crackpots. The conclusion of this essay will address the conflict between such a hypothesized inspired body public and the energy industry, in an attempt to offer some suggestions to overcome this oppositional dynamic.

Conclusions

Several conclusions can be drawn from the discussion herein. First, a perceptual differential exists between those within the energy infrastructure and the public. Based just on these differences in interpretations, but enhanced by galvanizing events, the results of perceptual differences can profoundly affect the short-term operations and the long-term viability of the nuclear energy industry. Failure to understand these existing and potential differences in perceptions can alter the social and political landscape, perhaps to the ultimate determent of the nuclear industry. What are some of the specific social and political circumstances that can be affected by such differentials?

The first dimension may well be technology. The industry has faith in its engineering and the technological controls that embody that faith. The everyday operation of so many plants across the world, generally without incidence, is testimony to that faith and the power of a belief in the industrial prowess of nuclear technology. The flip side of this is that when an incident occurs, the pre-exiting claims of safety and security come into question and defending technology during these times is problematic at best, and can be severely damaging to the industry's social and political image if not addressed with a critical assessment of where the critiques come from, what they represent, and why they persist over time.

The second dimension is that surrounding politics. In general, political structures are supportive of energy production; it is after all the fuel that drives financial expansion and provides for economic viability. The loss of faith by the body politic in nuclear energy can significantly affect the structures of power that are normally very supportive of the nuclear industry. The result may be a temporary or even permanent loss of such

structural support. The growth of a perceptual divide between industry and governments would be potentially devastating to one (energy industry) of these institutions and failure to address such perceptual disjunctions could damage the other.

The third dimension, social factors like alterations in the economics of power generation, loss of tourist revenue due to contamination perceptions, and many other socio-economic factors are equally troubling since they can inauspiciously impact the energy industry. Failure to recognize the reality of public fears about such factors, as well as the dismissal of those fears due to industrial/corporate arrogance, may be equally as ruinous for the long-term health of the energy industry.

Additionally several suggestions emerge from the analysis of public and industry perceptions. First, the industry should acknowledge that a perceptual difference exists and that it matters. This acknowledgement would start to allow for a more productive dialogue between the parties and about the very real issues that arise from such differences in perceptions. One social scientific based research methodology to assess the extent of the differences would be to conduct a survey of industry insiders on their perceptions of the nuclear industry and its importance to society. Comparison of these results to existing survey data on the public perceptions of the industry may yield critical one or more nexus of discussion between the two sides and suggest ways to bridge the gaps between the two perceptual endpoints they seem to represent. Once such disjunctions are identified by means of research, the industry and critical stakeholders from the critics of the industry could then shape public and industry awareness campaigns to educate both on the reasons for such disjunctions. Perhaps in this more inclusive way the two could shape a new and productive dialogue dynamic.

Nuclear power is a mature technology and its vital place is assured in many societies, unless the fears and perceptual divides noted above are neglected, forgotten, or plain ignored.[xviii] These offer serious challenges to the energy industry if its representatives foster disbelief in the industry, fail to take cautions from criticisms, and in general act with arrogant aforethought. Social perceptions are genuine and have very real social and political power when harnessed. The question is which side of this divide will harness them to their advantage during times of crisis. The nuclear power industry has some successes over the years, but the potential for failure is just a misperception away.

References

Abbey, E. 2000. *Monkey wrench gang*. New York: McGraw-Hill.

Berger, P. L. and T. Luckmann. 1967. *The social construction of reality.* Garden City, New York: Doubleday.

Farquhar, B. July 18, 2003. "Nuke train rolls, two years late." Casper Wyoming *Star Tribune.* Download date: August 13, 2003. Available: http://casperstartribune.net

Flavin, C. 1987. *Reassessing nuclear power: The fallout from Chernobyl.* Washington, DC: Worldwatch Institute.

Goldstein, R. L. and J. K. Schorr. 1991. *Demanding democracy after Three Mile Island.* Gainesville: University Press of Florida.

Goldstein, D. K., J. M. Wenger, K. V. Dillon, and D. M. Goldstein. 1999. *Rain of ruin: A photographic history of Hiroshima and Nagasaki.* Washington, DC: Brasseys.

Graham, J. D., J. B. Wiener, and C. R. Sunstein. 1997. *Risk verses risk: Tradeoffs in protecting health and the environment.* Cambridge: Harvard University Press.

Margolis, H. 1997. *Dealing with risk: Why the public and the experts disagree on environmental issues.* Chicago: University of Chicago Press.

Marples, D. R. 1988. *The social impact of the Chernobyl disaster.* New York: St. Martins Press.

Medvedev, Z. A. 1992. *The legacy of Chernobyl.* New York: W. W. Norton.

Mould, R. F. 2000. *Chernobyl record: The definitive history of the Chernobyl catastrophe.* Bristol: Institute of Physics.

Noble, D. F. 1993. *Progress without people.* Chicago: Charles S. Kerr Publishers.

Nuclear Regulatory Commission. 2002. *Fact sheet on the accident at Three Mile Island.* Download date: September 1, 2003. Available: http://www.nrc.gov.

Nuclear Regulatory Commission. 2000. *Fact sheet on the accident at the Chernobyl nuclear power plant.* Download date: September 1, 2003. Available: http://www.nrc.gov.

Oe, K. (T. Tonezawa and D. L. Swain translators). 1995. *Hiroshima Notes.* London: Marion Boyars Publishers. Ltd..

Pawelski, N. 1999. "Essay: Memories of a nuclear disaster." *CNN.com.* Download date: September 1, 2003. Available: http://www.cnn.com.

Perrow, C. 1999. *Normal accidents: Living with high risk technologies.* Princeton: Princeton University Press.

Sale, K. 1996. *Rebels against the future: The Luddites and their war on the industrial revolution.* Boulder: Perseus.

Schutz, A. 1967. *The phenomenology of the social world.* Evanston, Illinois. Northwestern University Press.

Schutz, A. and T. Luckmann. 1974. *The structures of the life-world.* London: Heinemann.

Slovic, P. 2000. *The perception of risk.* London: Earthscan Publications.

Struglinski, S. August 12, 2003. "Nuclear shipment shrouded in secrecy." *Las Vegas Sun*. Download date: August 13, 2003. Available: http://www.lasvegassun.com.

Tetreault, S. August 13, 2003. "Waste shipment raises concern." *Las Vegas Review Journal.* Download date: August 13, 2003. Available: http://www.reviewjournal.com.

Wood, M. S. and S. M. Shultz. 1988. *Three Mile Island: A selectively annotated bibliography, volume 4.* Westport: Greenwood.

[i] This essay will intertwine nuclear power production with its by-product issues: nuclear waste storage and disposal. The author's own work has advocated that the risks of terrorism against plants are equal to a potential attack on SNF storage facilities and/or an attack on in-transit radioactive waste shipments.

[ii] The author of this essay has almost ten years experience writing about the sociological and political aspects of security for nuclear waste transportation. His work has focused primarily on potential terrorism attacks against SNF transportation efforts to Yucca Mountain, Nevada, USA. The discussion herein is not technical in nature, rather it is more impressionistic and the arguments are social science based, at least the social interpretive variant. This argument is deliberately not based on probabilistic risk assessment or other typical communication means used within the nuclear infrastructure.

[iii] "Stonewalling" is the term used to denote a persistent refusal to grant critics legitimacy with respect to their arguments; a persistence in beliefs about the strength of existing safety and security arrangements in light of changing terrorist threats; and/or a political technique to outwait the opposition until the immediate crisis of legitimation passes and normalized energy production activities can be reestablished.

[iv] Risk perception is a field often associated with economics, insurance, and engineering and has specific meanings in each of these areas of scholarship. Risk in the sense used herein refers to social, economic, and cultural risk or what Graham, Weiner, and Sunstein (1997) refer to as the chances of adverse outcomes: to humans, to their lives and the quality thereof, and to the environment. The perception of risk is generally thought to be associated with: 1) the probability of something happening and 2) the consequences of that action if and when it does happen. In many cases these two factors produce disagreement (Margolis 1997), especially when discussing complex systems and complex technologies (Perrow 1999) like those surrounding nuclear materials and radioactive waste products.

[v] Generally the risk literature reflects three perceptual paradigms (Slovic 2000). The first paradigm is characterized as *absolute rationality* where the industry experts are considered most appropriate in making the calculations since they have the most relevant information on the subject of nuclear related risks. In this perspective the general public and those not inside the industry are considered irrational and thus their suggestions untrustworthy. The second, *limited rationality*, acknowledges that human ability to know every variable that may impact risk is not a realistic expectation. What is more pragmatic is to educate laypersons to understand the consequences of risky decisions with respect to key variables, thus this paradigm would seek to educate the populace as to the reasonableness of accepting the risks associated with nuclear power. The last paradigm is *social/cultural rationality* that refers to the perception wherein the public is not considered teachable on such highly technical matters. This then is considered a public good since to do so may reveal critical safety and security information. As an example, the United states department of Energy (DOE) recently conducted a shipment of nuclear waste from New York to Idaho (a 2300 plus mile trip) under a shroud of secrecy, or at least the public perceived the shipments thusly (Farquhar 2003; Tetreault 2003; Struglinski 2003). The original shipments of these fuel assemblies and their delivery was delayed by the events of September 11, 2003.

[vi] The opposition to the Yucca Mountain geological repository project has lasted decades and involved environmentalists, nuclear power opponents, local governments, and many other stakeholder groups. The best documentation of alternative perspectives on the Yucca Mountain project can be found at http://www.state.nevada.us/nucwaste/. This website offers various critiques of the project including those related to policy issues, legal issues, transportation related issues, socio-economic issues, health effects, and technical issues. Clearly, the State of Nevada's arguments do not rest merely on a single issue with the repository; this local government entity has fought the placement of the repository within its geographic boundaries on a variety of grounds and from many different perspectives over the course of the last few decades.

[vii] See testimonial record from the hearings before the *Committee on Energy and Natural Resources*, One-Hundredth Seventh United States Congress. "Testimony regarding S. J. Res.34 Approving the Site at Yucca Mountain, Nevada, for the Development of a Repository for the Disposal of High-level Radioactive Waste and Spent Nuclear Fuel, Pursuant to the Nuclear Waste Policy Act of 1982*"*. May 2002.

[viii] The idea of a social construction of reality comes from the work of Albert Schutz and others working in the tradition he helped to found. This tradition is commonly known as phenomenological sociology (Schutz 1967; Berger and Luckmann 1967; Schutz and Luckmann 1974). See the referenced literature for additional details on this theory and the 'life-world' concept discussion used herein.

[ix] The characterization that opponents to nuclear power use that equates nuclear power generation activities to the use of nuclear weapons is commonplace and subject to much negative dialogue from energy industry insiders. This negativity may be a common perception by nuclear industry insiders, at least when they fail to understand the perceptional differences this characterization represents. The same insiders may see that any opposition to their industry, by environmentalists and others, is based on this "misperception" and thus not worthy of their time and energy. When faced with long term and intense debates/criticisms on the social viability of nuclear power, the attitudes they posit can also become based on frustration. When this happens the attacks on the opposition can become polemical. It is as if the argument against nuclear power is so far removed from the nuclear industry experience, so detached from the insiders realities, that what many industry supporters feel at these times is articulated thusly: The (insert opposition – e.g., environmentalists) are against (insert characterization - e.g., progress) and they are (insert invective here – e.g., radicals). If you are interested in the history of Hiroshima see the essays of the Japanese writer Kentzaburo Oe (Oe 1995). To better understand a source of pop culture images associated with nuclear devastation see (Goldstein, Wegner, Dillon, and Goldstein 1999).

[x] For an example see the DOE's draft or final *Environmental Impact Statement* for the Yucca Mountain project. Details are available at http://www.state.nevada.us/nucwaste/.

[xi] One personnel example may help illustrate this point. When talking about the safety and security of nuclear waste transportation from Savannah River, Georgia (USA) to a DOE facility in Idaho, a safety expert directly involved in the shipment engaged in an intense debate and assured this author the safety and security of such shipments was paramount to him and his agency. The debate concluded with a definitive comment, at least for the security expert, to the effect that if he was not worried for the health and safety of his family, then the criticisms must be moot/irrelevant. This is illustrative of the disjunction in risk perception between those within the infrastructure and those held by outsiders. It may also be a good example of what has been termed total institutional socialization – where those within the industry have been so socialized by their employers and social relations within their job environments that nothing else can become a reality.

[xii] During the dawn of the industrial revolution groups formed that opposed technology and the progress it brought to humanity. The Luddite movement in England was one example of such a movement. In the early years of the 19th century opposition to technological advancement, the Luddites attacked especially that which displaced industrial workers who were flocking to cities for jobs. These technological advancements were targeted, both physically and intellectually. Some of the basic tenants of this movement were/are that technologies are never neutral and in many cases they represent harmful advancements for society; the nation state is intertwined with industrialism and can not be overthrown by revolt; and lastly, resistance to industrialization is not only possible, but desirable to offset this march of progress (Sale 1996). Contemporary articulations of this philosophy are known as neo-Luddite thought and in the computer dominated workplace of today the arguments have morphed to include the idea that society has become too reliant on technology and that we need to remember that technology is a servant of mankind, not its master. For examples of contemporary Ludditism inspired texts and arguments see (Abbey 2000; Noble 1993).

[xiii] The globalize operation of NPP are mostly incidence free and do not offer the level of threats most laypersons associate with this source of energy. That argument aside, the few high profile problems that arise, the problems associated with nuclear waste reprocessing and/or disposal, social movements advocating a progress away form nuclear power, and the unanswered question of safety and security in light of creditable terrorist threats against NPP, spent fuel pools, and waste shipments are problematic. Such threats, in some cases not yet a reality, are on the edges of the social radar since intelligence agencies have found some evidence of potential attacks and regulators such as the International Atomic Energy Agency (IAEA), Northern Atlantic Treaty Organization (NATO), and United States Nuclear Regulator Agency (NRC) have started to give such threats serious consideration. The security debates on NPP in the post-September 11, 2001 era are illustrative of these concerns (discussed elsewhere in this essay).

[xiv] For some written reflections on the TMI accident see recent memoirs from one reporter at the scene (Pawelski 1999) and some of the many books on the subject (Goldstein and Schorr 1991; Wood and Shultz 1988).

[xv] For more details on this accident see (NRC 2000; Mould 2000; Medvedev 1992; Marples 1988; Flavin 1987).

[xvi] The aftermath of these attacks were global and potentially profound as to nuclear power security and safety. In Australia the headlines read "Bomb scare at nuclear reactor" (*The Australian*, October 9, 2001); In Bulgaria "Bulgarian nuclear officials dismiss doubts about security at plants" (*BBC Monitoring Service*, October 1, 2001) while a few days later the headlines read "Additional security measures adopted at nuclear station" (*BBC Monitoring Service*, October 8, 2001); In Canada the headlines read "Security tightened at Canadian nuclear plants" (*The Star*, September 26, 2001); In Finland the story read "Finns consider possibility of terrorist attack on nuclear power plants" (*BBC Monitoring Service*, September 27, 2001); France may have had the most dramatic headlines: "France positions missiles to protect nuclear plant" (*The Guardian*, October 20, 2001); while in Germany the reports were equally dramatic "Nuclear reactors not made to withstand airborne terrorist attacks" (Schwobel and Thielbeer, *Allgemeine Zeitung*, Sept 27, 2001). Discussions along the same lines could be found in media coverage in Japan, Romania, Slovakia, Sweden, Switzerland, the United Kingdom, the United States, and other locations where NPP are located.

[xvii] The post-September 11, 2001 debates on nuclear waste and Yucca Mountain transportation security help illustrate this perceptual divide. On one side industry representatives downplayed the threats to NPP and waste shipments (see a *Science* article by Chapman et al 2002). This article was written by a large group of industry insiders and dismisses the possibility of an attack on a NPP and downplays the potential consequences of an attack against both NPP and waste shipments. The other side of the debate is embodied in the State of Nevada's long standing positions on transportation safety and security which suggest that prior to this attack severe security issues existed with SNF transportation planning and safety and that in the aftermath of the attacks on September 11, 2001 reconsideration would be prudent (see http://www.state.nv.us/nucwaste).

[xviii] The DOE's *International Energy Outlook* (2003) shows that as of 2002, 441 NPP were in operation around the world. In some geographic regions a decline in production can be seen, for example in many more developed nations like the United States and certain parts of Europe. Likewise in other regions of the globe an increase in production is noted, particularly in the developing world and Asia. See http://www.eia.doe.gov.

Review

Culture Shock: Securing the Bomb is Hard To Do

James E. Doyle
Nuclear Nonproliferation Division
Los Alamos National Laboratory

Hundreds of organizations throughout the world, from secret directorates within national armed forces to university engineering departments have the responsibility of keeping nuclear weapons or nuclear materials safe from theft or misuse. How well can they do this critical job? Are there legal requirements for certain measurable security standards? How do they develop and maintain "best practices?" Will they be shut down or have their nuclear materials confiscated if poor security is proven?

As highlighted by a recent landmark report, much depends on the quality and strength of the "security culture," within these organizations and the states that host them. The Center for International Trade and Security at the University of Georgia released its report "Nuclear Security Culture: The Case of Russia," in December 2004. The report asserts that even after more than a decade of technical and financial assistance from the West to improve the security of its nuclear weapons and materials, "Russia's nuclear sector will continue to require not only technological innovation, but also the cultivation of knowledgeable, skilled, and motivated personnel who are trained to use modern equipment and adhere to best practices." This is because as the report makes abundantly clear money and technology are not enough to produce good security. The quality of the "human factor" is key.

While Russia is the subject of the report, its basic conclusions are true around the world. In the era of "super terrorism" effective security cultures are critical to national and global security. As the report states "security culture, is a concept that encompasses a set of managerial, organizational, and other arrangements. Security culture connotes not only the technical proficiency of the people entrusted with security, but also their willingness and motivation to follow established procedures, comply with regulations, and take the initiative when unforeseen circumstances arise."

The report breaks new ground and exceeds its two primary objectives of further developing the concept of security culture and suggesting a comprehensive plan for building such a model within an organization. It provides the most comprehensive treatment of the issue to date and, using its thorough analysis of the Russian case, identifies clear actions that that can be taken to build a strong security culture in that nation and others.

The importance of this reports message cannot be overstated. Creating strong security cultures will require the commitment of resources, trained personnel and effective administrative and regulatory procedures that are difficult for many states to sustain. In

general, even the strictest security measures are vulnerable to forces and instabilities of the societies in which they operate. The many examples of security weaknesses and attempts to improve them at the national, facility and individual levels in Russia provided in the report make this especially clear.

Even when effective measures are in place, security can never be perfect. Moreover, there are presently no binding global nuclear material security standards or authority empowered to confirm that high standards are being implemented. The quality of security and accounting for nuclear weapons and materials varies greatly and is largely at the discretion of each state where these materials exist.

Given this unsettling reality "Nuclear Security Culture: The Case of Russia," makes a vital contribution to the literature and practice of nuclear security. It offers ten practical recommendations for Russian leaders and others to consider for improving nuclear security in Russia and four for how the international community can assist this effort in Russia and strengthen nuclear security culture across the globe. Two of the reports appendices provide powerful tools for designing actual programs and procedures that would benefit security at nuclear facilities. These are a model training curriculum to help managers begin the arduous task of nurturing security culture within their organizations a generic evaluation methodology to enable them measure their progress toward a healthy security culture.

The success of this report was assisted by the credentials and experience of the authors and contributors, several of whom have been working for many years directly and in conjunction with the U.S. National Nuclear Security Administration with officials and facility operators in Russia to improve security conditions. Peer reviewers included several prominent U.S. and Russian experts who have worked tirelessly to improve global nuclear security. All those with the responsibility and desire to prevent the unauthorized or malignant use of nuclear weapons and materials will benefit greatly from this report.

Research Paper (LAUR 96-2474)

The Ineffectiveness of the Correlation Coefficient for Image Comparisons *

Eugene K. Yen and Roger G. Johnston

Vulnerability Assessment Team

Los Alamos National Laboratory

MS J565, Los Alamos, New Mexico 87545

---

*Editor's Note: This paper has not been peer reviewed.

The Ineffectiveness of the Correlation Coefficient for Image Comparisons

ABSTRACT

Pearson's r linear correlation coefficient is widely used for comparing images. Image processing experts appear to be cognizant of its serious limitations. This information, however, has not been communicated well to non-experts (including those working on security applications), who sometimes use the correlation coefficient without being aware of its problems. We discuss the disadvantages of the correlation coefficient and show specific examples of strikingly poor performance in the context of security.

INTRODUCTION

Pearson's correlation coefficient, r, is widely used in statistical analysis, pattern recognition, and image processing [1-8]. Applications for the latter include comparing two images for the purposes of image registration, object recognition, and disparity measurement. For monochrome digital images, the Pearson correlation coefficient is defined as [1,4,7]:

$$r = \frac{\sum_i (x_i - x_m)(y_i - y_m)}{\sqrt{\sum_i (x_i - x_m)^2} \sqrt{\sum_i (y_i - y_m)^2}}$$

where x_i is the intensity of the ith pixel in image 1, y_i is the intensity of the ith pixel in image 2, x_m is the mean intensity of image 1, and y_m is the mean intensity of image 2.

The correlation coefficient has the value r=1 if the two images are absolutely identical, r=0 if they are completely uncorrelated, and r=-1 if they are completely anti-correlated, for example, if one image is the negative of the other.

The correlation coefficient is used for security applications such as surveillance, treaty verification, tamper detection using security seals, and tagging [9-14]. (Seals leave unerasable evidence of entry or tampering; tags are devices or procedures that uniquely fingerprint an object.)

Typically, the correlation coefficient is used to compare two images of the same object (or scene), taken at different times [11-14]. The r value indicates whether the object has been altered or moved.

In theory, we would obtain an r value of 1 if the object is intact, and a value of less than 1 if alteration or movement has occurred. In practice, distortions in the imaging system, pixel noise, slight variations in the object's position relative to the camera, and other factors produce an r value less than 1, even if the object has not been moved or physically altered in any manner [13]. In our experience with security applications, typical r values for two digital images of the same scene, one recorded immediately after the other using the same imaging system and illumination, range from 0.95 to 0.98. This is the same range as that reported by Palm and DeVolpi [13] for scanning electron microscope images.

Usually there needs to be an empirical definition of a threshold r value that indicates a breach of security. In other words, it is necessary to determine the minimum r value needed to conclude with confidence that the image is unchanged. For several security applications for which we are familiar, the chosen threshold values for r range from 0.30 to 0.85, depending on the application [9-14].

The purpose of this paper is to offer simple examples of the poor performance of the correlation coefficient for image comparison, particularly with security applications in mind. We know of no similar presentation. The problems and limitations of the correlation coefficient have been discussed previously [2, 3, 13-17], but briefly and abstractly, without specific image examples.

Furthermore, the knowledge that the correlation coefficient often performs poorly does not seem to have been communicated well to non-experts. We conducted a survey of 50 image processing texts, introductory through advanced, that discussed the correlation coefficient. Only 3 of the 50 texts discussed potential problems and limitations of the correlation coefficient, and then mostly in terms of its computational intensiveness, rather than performance problems.

STRENGTHS AND WEAKNESSES OF THE CORRELATION COEFFICIENT.

One of the obvious advantages of Pearson's correlation coefficient is that it condenses the comparison of 2 (often large) two-dimensional images down to a single scalar, r. Additionally, the correlation coefficient is completely invariant to linear transformations of x or y [1, 4, 13]. As a result, r is insensitive (within limits) to uniform variations in brightness or contrast across an image. Such spatially uniform variations can be caused, for example, by differences in the brightness of the light source over time, by changing background light levels, or by variations in the gain of the imaging system.

Despite its advantages, the correlation coefficient has many problems and limitations. The most widely recognized disadvantage is that it is computationally intensive. This often limits its usefulness for image registration (that is, orienting and positioning two images so they overlap). The correlation coefficient is also extremely sensitive to the image skewing, pincushioning, and vignetting that inevitably occur in imaging systems. Such distortions are particularly prevalent in scanning electron microscope pictures [13] because of the non-linearities and complexities of electron optics. (Image skewing occurs when an image slants in one direction. Pincushioning means that the edges of the image are concave. Vignetting is a reduction in the image intensity near the edges due to optical light collecting considerations.)

Another problem often overlooked in practical applications is that r is undefined--due to division by zero--if one of the test images has constant, uniform intensity. Users, especially for

automated security applications, must be careful that the computer or micro-processor doing the r calculations does not permit an undefined value to default to r=0 or r=1.

Other problems with the correlation coefficient include possible bias [16], complexities of interpretation [1], over-sensitivity to pixel noise and gain variations [2, 5, 15], difficulties in dealing with perspective or with moving illumination sources [2,15, 17], undesirable behavior for images containing too much fine structure or too little [2, 15], and trouble in dealing with images having strong spatial disparity gradients [2].

There is an additional problem with the correlation coefficient that does not appear to have been discussed or demonstrated in detail elsewhere. An image can be greatly modified, without this being detected, as long as the local mean and/or histogram of pixel intensities are relatively unchanged. This is demonstrated below.

EXAMPLES OF POOR PERFORMANCE

The top image in figure 1 shows an 8-bit (monochrome) 512 X 512 scanning electron microscope image of a metal surface. The complexity of the surface can be used as a unique identifier, or tag [13]. For the bottom image in figure 1, we have used a computer to artificially modify the top image such that the letters "LANL" replace a portion of the original image. The intensity for the letters was chosen such that the mean intensity of the region being overwritten did not change. Even though the human eye can immediately judge that the top and bottom images in

figure 1 are dramatically different, the correlation coefficient reports that these two images are essentially identical: r=0.94. This is about the same correlation coefficient one gets by re-recording a second image of the surface shown in the top of figure 1.

Figure 2 shows an even more disturbing example of the failure of the correlation coefficient to detect changes in an image. Recognizing that individual pieces are missing is critical for applications such as reflective particle tags (RPTs). These consist of small, highly reflective particles attached to an object. RPTs uniquely fingerprint the object based on their complex spatial distribution [12].

The top image in figure 2 is a monochrome 8-bit video image with 512 X 512 pixels. The image shows a collection of plastic-coated paper clips spread out randomly on a surface. The bottom image in figure 2 shows another image of the scene except that one of the paper clips has been physically removed prior to recording this second image. The dark paper clip missing from the bottom image in figure 2 can be seen slightly up and to the right of center in the top image. The correlation coefficient for the top vs bottom image in figure 2 is r=0.98.

Now one way to improve the performance of the correlation coefficient--and make it less sensitive to image skewing, pincushioning, vignetting, or imperfect registration--is to compute r over a subset region of the complete image [13]. Even this approach, however, can still produce poor performance. If only the region inside the rectangle in figure 3 is used to compute r, the value is still quite large: r=0.86. The correlation coefficient is thus still reporting an almost

unchanged image, even though the missing paper clip is a major feature inside the (200 X 200 pixel) rectangle!

Finally, in figure 4, the correlation coefficient fails to be useful for Elvis sightings. The two images are clearly different, yet r = 0.94. The bottom image was created by a superposition of the top image and an image of Elvis, such that the resulting local mean and histogram of pixel intensities were largely unchanged.

CONCLUDING REMARKS

In summary, the correlation coefficient often fails to find differences in images that are widely disparate. In the case of a security system utilizing the correlation coefficient, an adversary can modify an object or scene quite dramatically and yet still go undetected, especially if he approximately preserves the local intensity mean and/or intensity histogram. Of particular significance for security applications, the correlation coefficient often fails to detect missing objects within an image. Performance often improves only modestly if the correlation coefficient is computed for subset windows of the entire image.

Even when the correlation coefficient does perform acceptably, there are usually better algorithms for image comparison. Typically, the optimum choice of algorithms depends critically on general characteristics of the relevant images, and details of the application. One fact often

overlooked is that the use of human vision with a blink comparator [10, 18] can often dramatically outperform even very sophisticated computer algorithms.

ACKNOWLEDGMENTS

This work was performed under the auspices of the United States Department of Energy. Anthony Garcia, Phil Jacobson, and Chuck Mansfield provided valuable assistance and input.

REFERENCES

1. J.L. Rodgers, J. L. and W.A. Nicewander, "Thirteen Ways to Look at the Correlation Coefficient", American Statistician 42, 59-66 (1995).

2. M. Jenkin, A.D. Jepson, and J.L. Tsotsos, "Techniques for Disparity Measurement", CVGIP: Image Understanding 53, 14-30 (1991).

3. R.Y. Wong, E.L. Hall, and J. Rouge, "Hierarchical Search for Image Matching", Proceedings of the IEEE Conference on Decision Control, pp. 405-408 (December, 1976).

4. M. James, Pattern Recognition, John Wiley and Sons, New York (1988), pp. 36-40.

5. D.I. Barnea and H.F. Silverman, "A class of Algorithms for Fast Digital Image Registration", IEEE Transactions on Computers C-21, 179-186 (1972).

6. E.H. Hall, Computer Image Processing and Recognition, Academic, New York (1979), pp. 480-485.

7. W.H. Press, B.P. Flannery, S.A. Teukolsky, and W.T. Vetterling, Numerical Recipes in Pascal, Cambridge University Press, New York (1989), pp. 532-534.

8. J. Lee, "A Cautionary Note on the Use of the Correlation-Coefficient", British Journal of Industrial Medicine 49, 526-527 (1992).

9. R.G. Johnston and A.R.E. Garcia, "Vulnerability Assessment of Security Seals", Journal of Security Administration 224, 24-29 (1995).

10. R.G. Johnston, "The Real Deal on Seals", Security Management 41, 93-100 (1997).

11. D.S. Kupperman, A.C. Raptis, J.T. Dusek, R.G. Palm, S.H. Sheen, and S.E. Dorris, "Assessment of Tamper-Revealing Ceramic Seals", Argonne National Laboratory Report ANL/ACTV-90/5, DE91007793, (September, 1990).

12. G. Staehle (Editor), "DOE's Tags and Seals Program", Verification Technologies, U.S. Department of Energy Report DOE/DP/OAC/VT-92B, (October, 1992).

13. R.G. Palm and A. DeVolpi, "Plastic-Casting Intrinsic-Surface Unique Identifier (Tag)", Argonne National Laboratory Report ANL/ACTV-94/1 (April 1995).

14. A. DeVolpi, "Understanding Correlation Coefficients in Treaty Verification", Argonne National Laboratory Report ANL/ACTV-91/4 REVISED (February 1993).

15. M.A. Crombie, "Coordination of Stereo Image Registration and Pixel Classification", Photogrammetric Engineering and Remote Sensing 49, 529-532 (1983).

16. I.J. Good and E.P. Smith, "The Possible Bias of the Pearson Chi-Squared Test in Non-Equiprobable Cases", J. Statist. Comput. Simul. 19, 79-95 (1984).

17. R.A. Schowengerdt, Techniques for Image Processing and Classification in Remote Sensing, Academic Press, New York (1983), pp. 27-35, 47.

18. R.G. Johnston and A.R.E. Garcia, "Simple, Low-Cost Ways to Dramatically Improve the Security of Tags and Seals". CD-ROM Proceedings of the IAEA Symposium on International Safeguards, Vienna Austria, October 13-17, 1997.

FIGURES

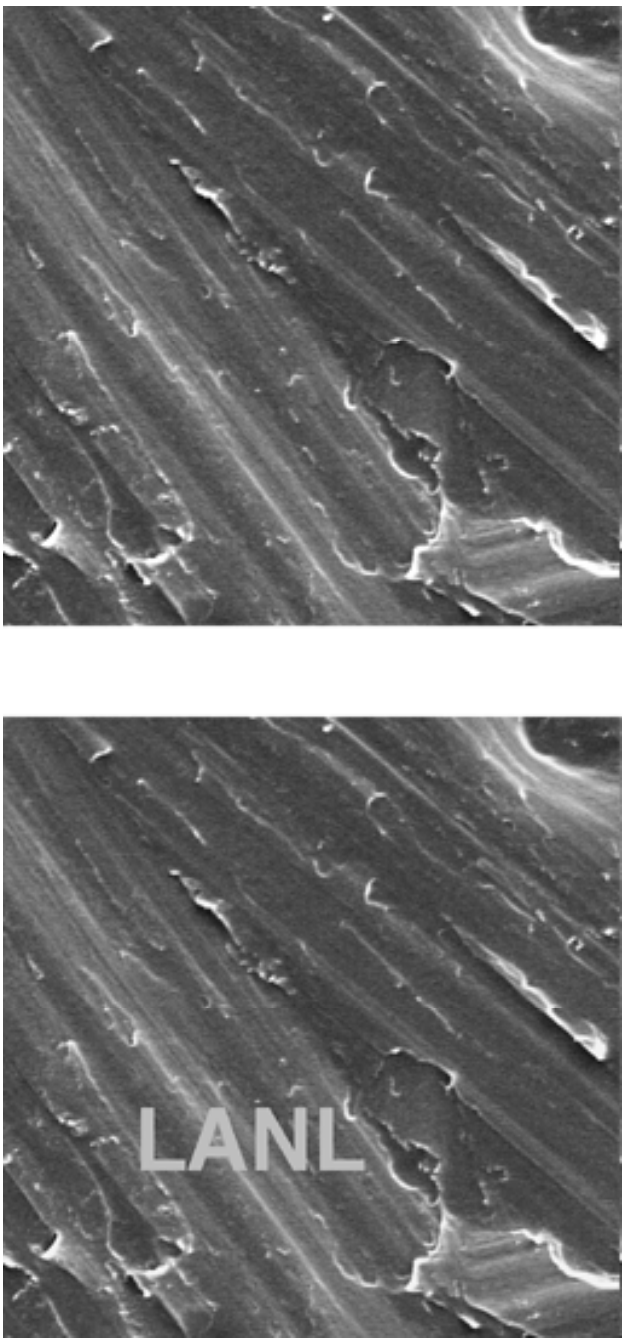

Figure 1. Comparing two images using the correlation coefficient. Both images are 8-bit, 512 X 512 scanning electron microscope images of a metal surface. The image at the bottom is the same as at the top except that the letters "LANL" have been overwritten. The pixel intensity of the letters is approximately equal to the local mean intensity of the original (top) image. The correlation coefficient for the top image vs. the bottom image is r=0.94. The correlation coefficient reports little difference.

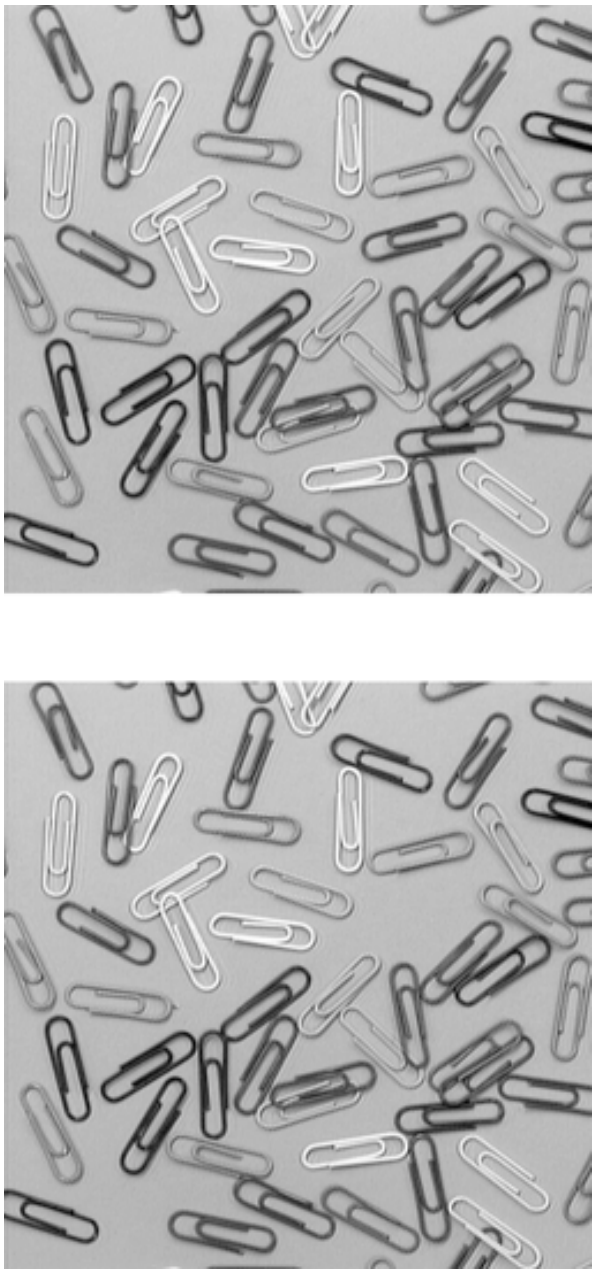

Figure 2. The correlation coefficient can be relatively poor at detecting missing objects in an image. Both the top and bottom images are 512 X 512 8-bit video images of plastic-coated paper clips. For the bottom image, one of the paper clips has been picked up and the image re-acquired. The missing paper clip is not detected: the correlation coefficient for the top image vs. the bottom image is r=0.98.

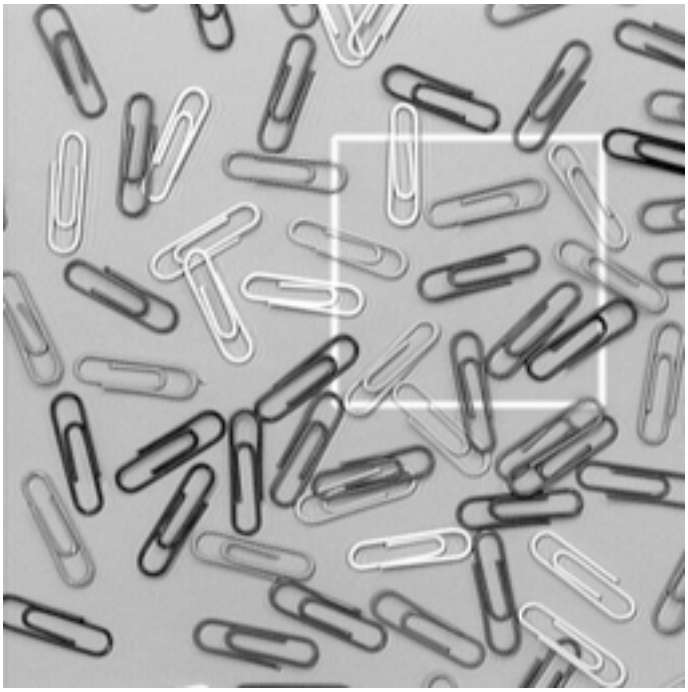

Figure 3. Reducing the window size only modestly helps the correlation coefficient detect the missing paper clip. If the correlation coefficient is recomputed for the top and bottom images in figure 2, limited to the subset (200 X 200) rectangle shown in this figure, then r=0.86.

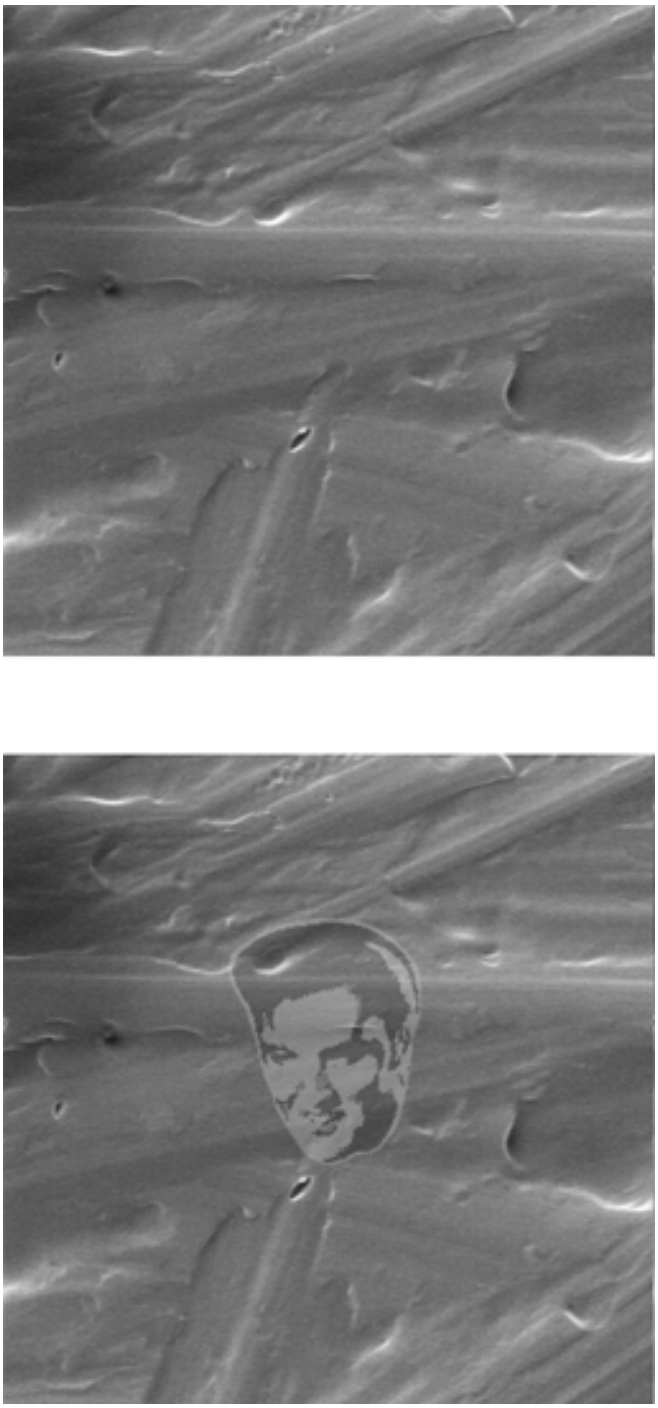

Figure 4. Scanning electron microscope images. The correlation coefficient fails to definitively detect the ghostly appearance of Elvis in the bottom image. For the top image vs. the bottom image, r=0.94.

Research Paper

Psychology in the Study of Physical Security*

Edward George Bitzer, III

Vulnerability Assessment Team

Los Alamos National Laboratory

and

Andrew Hoffman

Department of Psychology

University of Florida

---

*Editor's Note: This paper has not been peer reviewed.

Psychology in the Study of Physical Security

Considering the current global security environment the importance of good physical security is difficult to underestimate. And increasingly, physical security services are becoming a private rather than public service. According to the Bureau of Labor Statistics (2004), private security officers outnumber police officers by more than 2 to 1 in the United States. And increasingly, our society is relying on private firms to meet security needs. Recent reports suggest that this trend holds true for both daily security operations (Murphy, 1997) as well as times of crisis such as responding to terrorism (e.g. Virasami, 2005) or natural disasters (e.g. Higgins, 2005).

And while there is a large amount of research that has been conducted on policing, physical security has seen much less attention. The current state of research in the field of physical security could be described as fragmented or multidisciplinary, depending on your outlook. Physical security is primarily an applied field so, unlike areas like mathematics or physics, it has no dedicated line of research. Instead, the research that does exist is scattered through fields like engineering (both mechanical and electronic), computer science, chemistry and physics as well as social sciences such as criminology, sociology, and psychology. Multidisciplinary research can be healthy as it encourages new ideas and creative thinking, but too much fragmentation can be deleterious if physical security researchers are unable to find each other and share ideas. Exacerbating this fragmentation in the field of physical security is a lack of research outlets like peer-reviewed journals and academic conferences. Clearly there is a need for

outlets (such as this journal) where those active in the field of physical security can share ideas across specialty area. Which is what we hope to do with this article.

At its core, the act of providing security relies on two main elements, equipment or technology and people. And neither of these areas receives the attention and funding it deserves. But our experience suggests, although statistical proof was unavailable, that the lion's share of the funding that is available for research goes to equipment and technology. Some might say that such a distribution is merited because equipment is more important to security than people. Indeed, there seems to be a belief in the physical security world that there is some technological silver bullet that will solve security and eliminate the need for a human element at all. Others, however, would disagree. For example, General Eugene Habiger (ret.), former commander of U.S. strategic nuclear forces and security advisor to the U.S. Department of Energy has been quoted as saying "good security is 20% equipment and 80% people" (Bunn & Wier, 2004). While we suspect that both of these opposing views are partially right and partially wrong, the importance of the human element in good security should not be underestimated.

Consider this example drawn from one of the author's personal experiences. Not long ago this author lived in a condominium and apartment complex that had a contract with a private security firm to patrol the premises. There was a new puppy in the author's household and it happens that the firm's patrol schedule matched the puppy's schedule. As such, there were many occasions where the author was outside and had the opportunity to observe the duties preformed by the patrol officer. Essentially, it appeared that these duties simply involved driving to specified locations, jumping out of the patrol car and walking over to log the stop with a contact memory device attached to a fence,

and moving on to the next stop. This type of contact memory device scavenger hunt may be usefully in monitoring the movements of security officers, but it didn't make the complex more secure. These guards are so focused on getting to their pre-planned stops in a timely manner that security becomes less of a priority. Not once did those guards stop to ask how things were or if there was anything of concern they should know about. And their path to the corner of that fence and back into their patrol car was as predictable as the sunrise. In this case, the introduction of new equipment and technology (the contact memory device tracking system) actually hampered the job performance of the human elect (the security guards).

Of course we are not Luddites opposed to technology in any form, technology is a valuable asset in an overall security strategy. But we also believe that more attention needs to be spent trying to understand, and ultimately improve, the human elements of security. As such, the purpose of this paper is to point out lines of research into the human aspects of security that have not seen much attention but, in our opinion, deserve more. This is by no means a comprehensive list, and we could have included many other areas that we believe are fruitful. But rather than attempting the likely impossible task of developing a comprehensive list, we have focused on research in our areas of formal education (industrial/organizational psychology and social psychology for the first and second authors respectively) as well as those areas that might be especially influential or those that have been discussed frequently despite lacking much empirical research.

The Human Aspects of Physical Security

As we mentioned above, our rudimentary view of physical security breaks it down into two core elements. One the one hand there is equipment and technology and on the other is people. The people component of security might be further broken down into two subsets. The first subset contains issues and concerns that are purely human in nature and are associated with the impact that individuals, and groups of individuals such as organizations and societies, have on security. We will refer to this as the people component of security. The second subset contains issues and concerns associated with how humans interact with equipment and technology and how this interaction impacts security. We will call this the human factors of security. And while this division of the field of physical security is somewhat arbitrary, a comprehensive taxonomy of research in the field of physical security does not exist. In addition, the lines of research that we plan to discuss fall neatly into the two subsets above, so this division provides some structure for our discussion, to which we will now turn. What follows is a series of sections, each of which begins with a brief description of an issue in physical security and concludes with a discussion of theories and lines of research that could be brought to bear to help understand and address these issues.

The Human Factors Component of Physical Security

Increasingly, technology and advanced equipment are being utilized as a way to enhance security. However few, if any, security systems are completely automated. This means that at some point, the information collected by security equipment must be reviewed and acted upon by human security personnel. Consider the process of screening

baggage at the airport. Although x-ray machines may be helpful in speeding up the process, ultimately it is a person viewing images on a monitor that interprets the information the x-ray machines gather. In most cases, it is a human that makes key decisions about when to take action and what action to take. As such, it is the human component that must ultimately be deceived in order to breach security at such screening posts. And advances in technology including lower cost high quality video cameras, digital video recording and advanced imaging devises such as backscatter x-rays are making this type of setup very common outside of airports. More and more, the job of a security officer will be to watch a video screen for signs of trouble. Gaming security has relied heavily on security officers who specialize in video surveillance for some time and the proliferation of video cameras in recent years indicates that they are no longer alone.

However, prolonged monitoring of a video screen presents difficulties, which are often compounded by the fact that individuals usually monitor more than one screen at a time. Issues such as divided attention, prolonged attention, change blindness, visual fatigue and boredom all work to hinder performance in tasks such as these. Regrettably, we have seen little work on cognitive human performance issues such as these in the security research literature, although some research in this area has begun (Geraghty, 2003).

Fortunately cognitive performance questions like these have a long history in psychology. While many believe that the founder of psychology was Sigmund Freud, that honor actually belongs to a man named Wilhelm Wundt. In 1879, Wundt established the first known laboratory designed specifically for psychological research. It is worth mentioning this because Wundt's area of interest was sensation and perception, which is

an area ripe with theories that can be used to help explore many of the human performance issues in physical security.

Indeed, these theories have been applied to similar questions in the past. For example, since the early days of radar the military has been interested in how radar operators perform their job. To assist in understanding the process, researchers turned to signal detection theory (SDT). SDT (Proctor & Dutta, 1995) is essentially a way of determining an individual's ability to correctly distinguish a target signal (e.g. an enemy fighter) from background noise (e.g. birds, friendly planes, etc.). But the target in signal detection theory does not have to be an object, it could also be an event such as cheating at a gaming table. Regardless of what the target is, the use of SDT in experiments that systematically change aspects of the monitoring task (e.g. time on task, screens monitored, activity level around the participant) can help researchers to set up actual job conditions that support the desired level of vigilance among security officers. And since most of the work of security officers can be seen as monitoring tasks SDT could be applied to many other functions of security officers such as checking badges or authenticating the integrity of tamper-indicating seals.

The People Component of Physical Security

While it is difficult to asses the accuracy of Gen. Habiger's statement mentioned above, it would be equally difficult to argue that people are a wholly unimportant part of physical security. As such, it is worthwhile to pursue research aimed at understanding the role that people play in physical security. As was previously mentioned, however,

work in this area has been sparse. Nevertheless, there are a variety of issues in the field that could be successfully addressed through a better understanding of the human component of physical security. Therefore, we now turn our attention to outlining a sample of some of these problems and propose lines of research that may be helpful if applied to the field.

Security Guard Turnover

Employee turnover among security officers is, to put it mildly, alarmingly high. It has been estimated that turnover in the field may be as high as 100-300% in some cases (Castro, 2005; Roberts, J.R., 2003; Said, 2002). There is no shortage of authors in the field of physical security who have discussed the problems that this turnover creates (McNally, 2004). However, with few exceptions, proposed solutions to this problem seem to be lacking. Often (e.g. Goodboe, 2002; McNally, 2004) those proposed solutions seem to fall into what could be called the "why can't we all just get along" approach. Essentually, most of the solutions we have seen proposed involve no more than simply treating employees better. And while we have no doubt that treating employees well is important, we doubt that this approach alone will have a universal positive impact on reducing turnover. And such suggestions tend to be fairly amorphous in nature and are therefore can be difficult to implement. However, research on the phenomenon has revealed a number of specific interventions that may be helpful in reducing turnover among security officers (Bitzer, 2005a). Organizations in fields other than physical security have found that the use of employee selection programs such as personality

testing, biodata, and realistic job previews have been helpful in addressing this problem. Therefore, organizations that employ security officers may also benefit from applying these tools. Unfortunately, very little work has been conducted to assess the usefulness of these tools, so their actual impact is difficult to know for certain. As such, systematic evaluations of turnover reduction strategies such as these are badly needed and would be a fruitful area of research

Security Culture and Climate for Security

A more thorough discussion of security culture and climate for security can be found in this issue of the Journal of Physical Security (Bitzer, 2005b), but a brief mention is worthwhile here. Security culture could be defined as organizational manifestations which reflect the importance that an organization places on securing physical, electronic, and information assets. Climate for security, on the other hand, is employees' shared perceptions of what the organization is like in terms of security practices, procedures, routines, and rewards. When combined, both of these concepts work together to elicit appropriate security behaviors from employees. Organizations that value the importance of security and have artifacts (such as policies, procedures, and communication) which reflect these values are positioned to have a strong overall security environment. However, employee perceptions of such a culture will dictate they way they respond. All the security policies in the world are useless unless employees perceive them as appropriate and valuable. If they don't, security policies and procedures will likely be

ignored or circumvented. As such, shared employee perceptions (i.e. organizational climate) that support security are also important.

There has been an increasing interest in the concepts of security culture and climate for security in recent years. The International Atomic Energy Agency (IAEA) (IAEA, 20001; IAEA, 2002; IAEA, 2003; IAEA 2004), Presidents Bush and Putin (White House, 2005), and independent researchers (Khripunov, 2005a; Khripunov, 2005b; Khripunov, Nikonov, & Katsva, 2004) have all stated or eluded to the fact that the establishment of organizational culture and climate that supports security may be helpful to promote appropriate security behaviors among employees. While the concepts of culture and climate have been applied to enhance desired organizational outcomes such as safety (e.g. Zohar, 2000) and innovation (e.g. Stokols, Clitheroe, & Zmuidzinas, 2002), there has been little work attempting to apply these concepts to security. Therefore, there are still a number of untested, and thus unanswered, questions about the application of these concepts to security. Questions about the dimensions that comprise these constructs, the appropriate way to assess the concepts in a security context, and the generalizability of the concepts to a variety of security situations all need to be explored. While some work has begun to address these questions, much work still needs to be done. We strongly encourage others to take up the issue because progress will only be made when a committed and multidisciplinary group of individuals can come together and systematically begin to examine the topic.

Disgruntled Employees

It is a commonly held belief that the insider threat is a major, if not *the* major, concern when considering physical security (Johnston & Bremer-Maerli, 2003). And while there are a number of reasons why an insider may turn against their organization (Shaw, Post & Ruby, 1999), employee disgruntlement is likely high on that list. Indeed, there are a number of anecdotal examples of disgruntled employees who have acted in ways that have harmed their organizations (Shaw, Post & Ruby, 1999).

The problem of employee disgruntlement is serious and needs to be addressed. There is a significant amount of research on programs that attempt to counter employees' feelings of disgruntlement. Interventions such as whistleblowing programs, dispute resolution programs, and the use of ombudsmen all may be helpful. However, the impact of such programs on security is not well known and is worth examination. Sadly, some employees will experience disgruntlement regardless of what the organization does to counter such feelings. Thus, appropriate ways of identifying such employees and dealing with them must also be explored.

Professionalism

Some authors in the field of physical security (e.g., Goodboe, 2002; Somerson, 2005) stress the importance of possessing a professional attitude on developing a strong guard force. Indeed, psychological research outside of the field of physical security has demonstrated that attitudinal professionalism is significantly related to desirable outcomes such as a reduction in turnover intentions and an increase in job performance

(e.g. Bartol, 1979). Unfortunately security officers, unlike their counterparts such as police officers and fire fighters, tend to have a low level of professionalism.

Hall (1968) proposed five components of attitudinal professionalism that include: (1) the use of the professional organization as a major reference; (2) a belief in service to the public; (3) a belief in self-regulation; (4) a sense of calling to the field; and (5) autonomy. These subcomponents of professionalism are ripe for research in relation to security guards. The impacts of these components on security officers, ways to enhance professionalism among security officers, and related topics should all be explored.

Job Characteristics

Certain characteristics of the job that security officers perform present unique problems. While there are a number of such characteristics, we will briefly explore two that are somewhat related, namely boredom and performance appraisal.

We have already briefly mentioned the problem of boredom when discussing issues with video surveillance. However, boredom among security officers is not restricted to this type of task. Indeed, problems associated with boredom among security officers one patrol have been discussed in other research (Charlton & Hertz, 1989). Boredom becomes a problem for security officers because there are often only a limited number of incidents to which guards must respond. As a result, guards often end up sitting around for days, weeks, or months waiting for something to happen. And while this lack of security incidents is a good thing from the perspective of security, the boredom which results can have real negative outcomes. For example Wallace,

Vodanovich, and Restino (2003) found that high boredom proneness is associated making mistakes in accomplishing common tasks. As well, boredom proneness is associated with physical aggression, verbal aggression, anger, and hostility (Rupp & Vodanovich, 1997). Therefore, research on ways to reduce boredom associated with the job of security officers, as well as ways to select employees who are less prone to boredom, would be beneficial.

A related concern that we have about the job of security officers is the efficacy of performance appraisals. A common cliché about performance appraisal is "you get what you measure." If this is in fact the case, and we believe that it is, good performance appraisal is an important aspect of any job. However jobs like that of security officers, which have a low base rate of events, create problems in assessing performance. As a result, it is common to assess the performance of security officers by testing them on their knowledge of policies and procedures (Charlton & Hertz, 1989). While this might be useful for in assessing some aspects of job performance, it does not give a complete picture. Given this, novel ways of assessing the performance of security officers need to be proposed and tested.

Conclusion

Clearly there are a number of issues and concerns in the field of physical security that have yet to be explored in a systematic way. And many of these issues and concerns relate to the human side of the field. While we have identified some of these areas, there are many others which could have been discussed (e.g. security training, management

support for security, etc.). Fortunately, academic disciplines such as psychology and sociology are mature fields which have examined many of these issues in other contexts. We believe that the application of theories and propositions from these, and other, fields can be used to better understand and enhance the field of physical security. Hopefully the discussion above will spark more discussion of these and other concerns and ultimately lead to an increase in research on these topics.

References

Bartol, K. M. (1979). Professionalism as a predictor of organizational commitment, role stress, and turnover: A multidimensional approach. *Academy of Management Journal*, 22(4), 815-821.

Bitzer, E. G. (in press, 2005a). Security Staff Turnover: Situation Serious, But Not Hopeless. *Security Management*, Dec.

Bitzer, E. G. (2005b). Understanding and Applying Security Culture and Climate for Security in a Nuclear Environment. *Journal of Physical Security, 2*, pp

Bunn, M., & Wier, A. (2004). *Securing the bomb: An agenda for action*. Cambridge, MA: Harvard University, Belfer Center for Science and International Affairs.

Castro, H. (2005). Seattle council backs security guards' push for better training, benefits. *Seattle Post-Intelligencer*. Retrieved August 27, 2005 from http://seattlepi.nwsource.com/local/211146_security08.html.

Charlton, J. & Hertz, R. (1989). Guarding against boredom: Security specialists in the U.S. Air Force. *Journal of Contemporary Ethnography, 18*(3), 299-326.

Geraghty, C. L. (2003). Homeland security. *360 Magazine*, Summer, 18-23.

Goodboe, M. E. (2002). How to turn around turnover. *Security Management*, Nov., Retreived October 10, 2004 from www.securitymanagement.com/library/001336.html

Hall, R. H. (1968). Professionalization and bureaucratization. *American Sociological Review*, 33(1), 92-104.

Higgins, M. (2005, September 10). Katrina-hit states turn to security firms. *The Washington Times.*

International Atomic Energy Agency: Board of Governors. (2001, August). *Nuclear verification and security of material: Physical protection objectives and fundamental principles* (GOV/2001/41). Vienna, Austria.

International Atomic Energy Agency: Board of Governors/General Conference. (2002, September). *Measures to strengthen international cooperation in nuclear, radiation, transport and waste safety: Implementation of the revised action plan for the safety and security of radiation sources* (GOV/2002/35/Add. 1 – GC46/11/Add. 1). Vienna, Austria.

International Atomic Energy Agency: General Conference. (2003, August). *Nuclear security: Measures to protect against nuclear terrorism* (GC47/17). Vienna, Austria.

International Atomic Energy Agency: Board of Governors/General Conference. (2004, August). *Nuclear Security: Measures to protect against nuclear terrorism* (GOV/2004/50 – GC48/6). Vienna, Austria.

Johnston, R. G. & Bremer Maerli, M. (2003). The negative consequences of ambiguous "safeguards" terminology. *INMM Proceedings*, Phoenix, AZ.

Khripunov, I. (2005a). A cultural approach to improving chemical security. *The Monitor, 11*(1), 12-15.

Khripunov, I. (2005b). Nuclear security: Attitude check. *The Bulletin of the Atomic Scientists, 61*(1), 58-64.

Khripunov, I., Nikonov, D., & Katsva, M. (2004). *Nuclear security culture: The case of Russia*. Khripunov, I., & Holmes, J. (Eds.). Athens, GA: University of Georgia, Center for International Trade and Security.

McNally, S. W. (2004). Turn away turnover. *Security Magazine*, Sept., 16-20.

Murphy, J. P. (1997). The private sector and security: A bit on BIDs. *Security Journal*, 9, 11-13.

Proctor, R. W. & Dutta, A. (1995). *Skill acquisition and human performance* (pp. 33-38). Thousand Oaks, CA: Sage.

Roberts, J.R. (2003). *Quis custodiet ipsos custodes?: Who will guard the guards?* Retrieved August 26, 2005 from www.JRRobertsSecurity.com.

Rupp, D. E. & Vodanovich, S. J. (1997). The role of boredom proneness in self-reported anger and aggression. *Journal of Social Behavior & Personality*, 12(4), 925-936.

Said, C. (2002). Security Lapse: Private guards get little training and low pay, study says. *San Francisco Chronicle*. Retrieved August 27, 2005 from www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2002/06/11/BU172056.DTL&type=printable.

Shaw, E. D., Post, J. M., & Ruby, K. G. (1999). Inside the mind of the insider. *Security Management*, Dec. Retreived on August 30, 2004 from *http://www.securitymanagement.com/library/000773.html*

Somerson, I. S. (2005). Insight about outsourcing. *Security Management*, March, 73-77.

Stokols, D., Clitheroe, C., & Zmuidzinas, M. (2002). Qualities of work environments that promote perceived support for creativity. *Creativity Research Journal, 14*(2), 137-147.

U.S. Department of Labor: Bureau of Labor Statistics (2005). *May 2004 National Occupational Employment and Wage Estimates: Protective Service Occupations*. Retrieved April 13, 2005 from http://stats.bls.gov/oes/current/oes_33pr.htm

Virasami, B. (2005, April 28). City to train private security guards. *Newsday*, p. A17.

Wallace, J. C., Vodanovich, S. J., & Restino, B. M. (2003). Predicting cognitive failures from boredom proneness and daytime sleepiness scores: An investigation within military and undergraduate samples. *Personality and Individual Differences, 34*(4), 635-644.

White House: Office of the Press Secretary. (2005). Joint statement by President Bush and President Putin on nuclear security cooperation. Retrieved May 26, 2005 from http://www.whitehouse.gov/news/releases/2005/02/20050224-8.html

Zohar, D. (2000). A group-level model of safety climate: Testing the effect of group climate on microaccidents in manufacturing jobs. *Journal of Applied Psychology, 85*(4), 587-596.

Research Paper

Creative Adversarial Vulnerability Assessments*

Edward G Bitzer III and Roger Johnston
Vulnerability Assessment Team
Los Alamos National Laboratory

*Editor's Note: This paper has not been peer reviewed.

> *If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle. -- Sun Tzu*

During a press conference in May of 2002, then National Security Advisor Dr. Condoleezza Rice discussed the failure of the government to predict attacks similar o those that occurred on September 11, 2001. She stated that "I don't think anybody could have predicted that these people would take an airplane and slam it into the World Trade Center, take another one and slam it into the Pentagon; that they would try to use an airplane as a missile…"[1] Of course, that is exactly what happened. However, this paper is not meant as an indictment of the statements or ability of Dr. Rice, we use this example only because it is indicative of a greater problem among the United States intelligence/security communities and, we believe, the private security community as well. That problem, stated simply, is a lack of imagination. Indeed, the 9/11 Commission has also lamented such shortcomings. In their final report, the Commission succinctly states, "Imagination is not a gift usually associated with bureaucracies…It is therefore crucial to find ways of routinizing, even bureaucratizing, the exercise of imagination." To that end, we wish to share tools

[1] According to her testimony to the 9/11 Commission Dr. Rice commented about this statement. In her testimony Dr. Rice acknowledged that she had implied that no one could have imagined the threat of terrorists using planes as missiles. However, also in her testimony, Dr. Rice backed away from such statements saying "As I said to you in the private session, I probably should have said, 'I could not have imagined...'" such attacks. Retreating from such a statement was of course necessary because within days of Rice's initial comments at the May 2002 press conference, reports began to emerge that that someone *had* imagined such attacks. In fact, many such someone's had imagined such attacks including the intelligence community (in response to information about Libyans with similar plans for attacks on the WTC), Philippine authorities (who were told of plans for such attacks on CIA headquarters), a Justice Department lawyer, NORAD, Eric Harris and Dylan Klebold (the perpetrators of the Columbine High School massacre, and perhaps any number of Navy veterans who had experienced very real attacks of the same nature at the hands of Japanese Kamikaze pilots.

and techniques that may be helpful in brining the power of imagination to bear on the problems associated with security.

The authors of this paper are members of the Vulnerability Assessment Team (VAT) at Los Alamos National Laboratory. One major function of the VAT is to, as the name implies, conduct vulnerability assessments (or red teaming) in an attempt to discover weaknesses in physical security policies and procedures. In the course of these assessments, we strive to examine security not from the viewpoint of security professionals, but rather to put ourselves in the position of our adversaries. To think like the bad guys. And it is through this process (what is called *adversarial* vulnerability assessment), that we believe some of the most effective vulnerability assessments can be conducted. A full description of the 13 steps of the adversarial vulnerability assessment (AVA) process can be seen in an article written by Johnston (2004), and a full recitation of this process is beyond the scope of this paper. Instead, we will focus primarily on Step Four in that process. Johnston has identified this step, Brainstorming, as perhaps the most crucial step in conducting a successful vulnerability assessment. When this step is done well, an AVA can be a powerful tool for revealing major unforeseen vulnerabilities. When done poorly, AVA's are rendered no more useful than more traditional security walkthroughs.

Although this step has been called Brainstorming, the name can be somewhat misleading. In fact, the process can be viewed more broadly. Brainstorming is a particular technique (likely familiar to many) that can be very useful, but it is only one of a series of techniques that can be employed to come to the same ends: thinking imaginatively, or creatively, about potential vulnerabilities that might be present. It is a discussion of a series of these techniques that we will now turn.

Techniques for Thinking Creatively

Although it is somewhat novel in the security world psychologists, marketers and others have long been interested in ways to help teams of individuals to develop "outside-the-box" thinking. Through the course of this interest, a number of different ideas have developed. One of the first is the concept of brainstorming mentioned earlier. Others are variations, or evolutions, of the brainstorming concept. We hope to outline examples from each of these areas, as well as propose techniques not traditional thought of as creativity techniques, but which – when approached with the same sort of open-mindedness – can lead to similar results. As with the work of creativity theorists, we will start with brainstorming.

Brainstorming – There are a number of different writers and consultants who have promoted brainstorming as the answer to inducing creativity from a team. And it may be that there are as many processes of brainstorming as there are proponents. We are not especially convinced that any one process will be any more successful than any other. The bottom line is that most of these processes contain many of the same basic underlying traits. And it is our belief that as long

as these traits are present, any process of brainstorming can be successful. Therefore, it is vital that any team leader, in this case VA team leaders, know what the underlying traits are, and apply those traits in a way that makes sense for their particular team. As such, we will outline the four basic traits for brainstorming so vulnerability assessors can use them in appropriate ways.

1) Establish an objective – Objectives are important for any number of activities, and brainstorming is no exception. The purpose of establishing objectives is to set a clear expectation of what the brainstorming session is intended to accomplish. The purpose of brainstorming is to allow the brain to run wild with ideas, but the ideas still must be directed to a particular cause. Objectives establish that cause and keep everyone on the same page. Remember, we are talking about an adversarial vulnerability assessment. As such, the right type of objectives would be something like, “The goal is to attack X facility” or “We are attempting to create havoc in Z community.” We know that this may feel very alien and uncomfortable for individuals who have spent their lives and careers attempting to prevent such attacks, but the objective must focus on compromising a particular building, security device, etc. It is our goal to “know” our enemy, as in the quote above from Sun Tzu. It may also be helpful to establish a time limit for the session. This helps the team members, and the team leader, keep the team on track and moving forward toward successfully completing an objective.

2) Lay out ground rules – There are a number of ground rules that should be put in place in order to allow for the most effective brainstorming. The first is to identify a recorder who will write down all ideas. The ideas should be written down in full view of everyone (such as a chalkboard, whiteboard, or flip charts). This serves two purposes including preventing, to the extent possible, the repeat of ideas and to allow individual members to work off of others’ ideas. Second, there should be no judging of any of the ideas that are generated, no matter how absurd they may appear. Many great ideas throughout history, including that the world is round or the personal computer, have at one time been viewed as crazy. The most effective way to stifle creative thinking is to judge ideas during the idea generation phase. Criticism and judgment will cause participants to be less likely to go out on a limb and bring up what may potentially be valuable ideas. Third, eliminate all distractions including cell phones, pagers and the possibility that anyone not in the brainstorming session could interrupt. Brainstorming works best when one idea can flow fluidly from another, distractions will make that impossible. All participants should shut off electronic communication equipment and it might be helpful to hold the

session somewhere away from traditional meeting areas. You want team members to think outside-the-box so get them outside the office.

3) Generate ideas – This is the meat of the brainstorming session. It is at this point that, as mentioned previously, there are a number of ways to go about this process. Perhaps a free-flow of ideas, with no order of who can speak and when, will work best. Perhaps all participants should be given a few minutes to share their ideas, with time afterwards for anyone to share additional ideas they have thought of as others were speaking. Maybe you will require that all participants give at least one idea, maybe no such requirement is made. The key, however, is that the team leader select the procedure which best fits the personalities of their team. Fit, however, does not always mean making everyone feel comfortable. You want the team to feel safe to share ideas, but the point is to get them to stretch to find interesting, viable, and novel ideas.

4) Select ideas – At this point, it is hoped, there will be a number of ideas that have been generated. Most likely, more ideas than can reasonably be dealt with. Therefore, a process of selecting which potential attacks to examine in more detail must take place. Criteria for selecting where to focus may be on the ease with which an attack could take place, the consequences if such an attack were to occur, some combination of these criteria, or other criteria altogether. It may be beneficial to allow group members to become proponents of one or a few ideas in order to more fully consider all alternatives (the group leader, especially a powerful or well respected leader, should refrain from this process as he or she may exert undue influence and cause groupthink to take hold). Finally, each group member should be given one or more votes to cast for the idea that they think deserves the most consideration. The ideas that receive the most votes should become the focus of the remainder of the AVA.

Nominal Group Technique – The nominal group technique (NGT) is an evolution on the traditional concept of brainstorming. The NGT technique was developed as a way to avoid some of the pitfalls of group work, such as social loafing and the desire for anonymity. Social loafing is the tendency for individuals within a group to exert less effort to a particular task than they would if they were working alone. Anonymity is of particular concern in the security field. For a variety of reasons, there is often a “shoot the messenger” response to those that surface concerns about security procedures and plans. NGT attempts to address these and other brainstorming issues by first requiring that team members conduct brainstorming sessions individually to develop as many ideas as they can. Then they submit their ideas, sometimes anonymously, to a central recorder who

writes down everyone's ideas. It is only then that the whole group gets together to consider and evaluate each idea. Then the group as a whole will choose to accept ideas (or perhaps a combination of ideas) for the AVA. This selection process is often conducted in much the same way as the selection process in a brainstorming session.

SWOT Analysis – The process of conducting a SWOT analysis is probably very familiar to individuals with any management or strategic planning experience. A SWOT analysis gets its name from the four individual components that go into the analysis process. These four components are: strengths, weaknesses, opportunities, and threats. The basic idea behind a SWOT analysis is to identify areas that would fit under each of these four components, and then put each of these components together to find productive avenues for action. Although SWOT analysis is a fairly traditional strategic analysis technique, using it as part of an AVA is very untraditional. So we will describe in more detail how to conduct a SWOT analysis from an adversary's perspective.

1) Strengths – The first step in conducting an SWOT analysis is to identify the areas that are particular strengths to an organization (in this case the strengths of the adversary). Strengths are identified as internal to the organization. Examples of such strengths would include technical competence, an unblemished criminal background, or the ability to physically blend in with a crowd or their surroundings.

2) Weaknesses – The second part of the SWOT analysis is to identify weakness areas that the adversary might experience. Like strengths, weaknesses are internal areas within the organization. Examples of such weaknesses might include a tainted criminal background, the lack of appropriate access control metrics (e.g. keys, cards, passwords, or biometrics), or poor funding.

3) Opportunities – Third, one must identify the particular opportunities that exist for the adversary. Unlike strengths and weaknesses, opportunities are those areas that are external to the adversary, but in their operating environment. Examples of such opportunities might include knowledge of a particular timeline or planned route for the transfer of a valued commodity, knowledge of a particular type of access control system or guard schedule being used the target organization (your organization), or even a knowledgeable individual inside the target organization who could be bribed or coerced into giving valuable information.

4) Threats – The final step in the identification phase of the SWOT analysis is the identification of threats that the adversary might face. Like the opportunities, these would be in the adversary's

operating environment. Examples of threats might include such things as a well-trained and well-armed guard force at the target organization, police or intelligence services actively pursuing them, or an insider sympathetic to the adversary's target who may reveal their plans.

The second phase in the SWOT analysis is to combine the S's and W's with the O's and T's into a matrix. This process will create four strategy areas that can help in identifying the most valuable avenues for identifying potential adversarial action. The four strategy areas created include S-O strategies, S-T strategies, W-O strategies, and W-T strategies and would be presented in a form similar to the matrix below.

	Strengths	Weaknesses
Opportunities	S-O strategies	W-O strategies
Threats	S-T strategies	W-T strategies

S-O strategies outline particular areas that the adversary may be interested in exploiting. For example, high technical competence plus knowledge of particular access control systems might afford the adversary an opportunity to defeat such systems. S-T strategies indicate ways in which an adversary may use some of its strengths to help alleviate the potential impact of external threats. For example, using the ability to blend into their surroundings as a way to prevent confrontation with a well-armed guard force. W-O strategies provide the adversary guidance on ways to develop their internal organization to exploit a potential opportunity. An example would be gathering funds (which currently don't exist) in order to pay a knowledgeable insider for valuable information. Finally, W-T strategies identify the particular areas where an adversary would develop defensive plans for preventing the two areas from coming together. An example would be only recruiting or using operatives with clean criminal backgrounds, those who would not draw the attention of police or intelligence agencies.

After developing the particular strategy areas, from the perspective of the adversary, VA teams can develop counter-measures of their own to exploit actions that might be taken by an adversary. One possible example would be varying access control systems or layering systems on top of each other to prevent or deter adversaries from using those areas in an attack.

Conclusion

We believe that through use of the techniques described above, as well as any other technique that allow vulnerability assessors to think creatively, or imaginatively as the 9/11 Commission might call it, it is possible to conduct

vulnerability assessments that are powerful tools in discovering and alleviating potential vulnerabilities that might exist. And although AVA is not the only tool that can be used to attempt to strengthen security, when used in combination with more traditional techniques such as security surveys and risk management practices, a more secure environment can be created.