Argonne NATIONAL LABORATORY

# The Journal of Physical Security

Volume 6(1), 2012

JPS

## THIS ISSUE...

**Table of Contents**

***Journal of Physical Security*, Volume 6(1), 2012**

## Editor's Comments

Welcome to volume 6 of the Journal of Physical Security. This issue has papers about Fukushima implications, lock bumping, tamper-indicating seals, election security, stresses on windows for explosions vs. projectiles, and private security in Serbia and in Nigeria.

As usual, the views expressed by the editor and authors are their own and should not necessarily be ascribed to their home institutions, Argonne National Laboratory, or the United States Department of Energy.

*****

An intriguing article by Charles Kenny in *Bloomberg Businessweek*, entitled "Airport Security is Killing Us" makes several interesting points. Of the 150,000 murders in the U.S between 9/11 and the end of 2010, Islamic terrorists were responsible for fewer than 36. Outside of Iraq and Afghanistan, the total number of deaths due to Islamic terrorism was 200-400 worldwide in the same time period, about the same number that die *each year* in bathtubs in the U.S.

U.S. Government spending on homeland security between 2002-2011 was about $580 billion (not counting wars in Iraq and Afghanistan) vs. an estimated $123 billion economic impact of the attacks on 9/11.

While not a single terrorist has been caught trying to board an aircraft in the U.S. by airport screeners, hundreds of Americans have died since 9/11 because they drove in motor vehicles (much more dangerous than flying) to avoid onerous personal and baggage screening at airports.

For more information see http://www.businessweek.com/articles/2012-11-18/how-airport-security-is-killing-us.

*****

The controversy early this year on whether to block the publication of research on how to mutate H5N1 bird flu viruses into more pathogenic forms was certainly an interesting issue in physical security. For more information, see http://www.bbc.co.uk/news/health-17914706

*****

Want to spoof DNA biometrics? Check out the 1997 science fiction movie *Gattaca*. Or for $599 you can replicate DNA on a Mac, Windows, or Linux platform in a few hours. The OpenPCR or "Personal PCR Machine" (http://openpcr.org) automatically runs through the various heating and cooling cycles that are part of the Polymerase Chain Reaction (PCR) process routinely used by biologists and forensics experts to turn a very small DNA sample into a (relatively) large sample of identical DNA. *Wired* magazine gave the device mixed reviews (January 2012 issue, page 48).

A biometric that almost anybody can easily replicate is not much of a biometric! Unfortunately, we're somewhat in the same situation with most (all?) other biometrics.

*****

Sociologist and political scientist James Q. Wilson (1931-2012) died earlier this year. Wilson helped to advance our understanding in a number of areas of interest to physical security. His 1975 book, *Thinking About Crime*, put forth the theory that criminals might not be deterred by longer sentences, but that putting them behind bars could ultimately reduce crime simply by getting them off the streets.

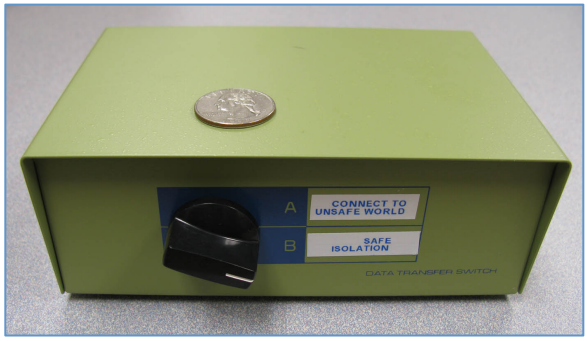
Wilson, along with George L. Kelling, devised the "broken window theory" that became the foundation for CPTED—Crime Prevention Through Environmental Design. The original concept appeared in their article, "Broken Windows" in the March 1982 edition of *The Atlantic Monthly*.

Then in 1989, Wilson wrote the classic tome *Bureaucracy*, a topic many physical security professionals are intimately familiar with. *Bureaucracy* was a kind of anthropological—and ultimately pessimistic/depressing—study of bureaucrats and bureaucracies.

Wilson's critics claimed he underestimated in his work the importance of civil liberties and civil rights. There is no doubt, however, that he was an original thinker who changed the mental landscape of how people view government, society, and security.

*****

Want to double your computer security for under $12? Get a RJ45 AB switch box. This makes it easy to disconnect from the Internet when you don't need to be connected, and instantly re-connect when you do. No fumbling with cables or software to disconnect/reconnect the Ethernet port. (Of course this doesn't address wifi or Bluetooth connections, nor help all that much if you are being personally targeted by hackers, but it can potentially cut down on opportunities for mischief.)




Front


Back

*****

Security professionals often must make difficult hiring decisions. Unfortunately, choosing good employees is still very much an art, rather than a science.

I was reminded of this by looking at the (surprisingly weak) correlation between an individual's success in professional football and how high he was chosen in the NFL draft. Now there are always injuries and unexpected situations that can limit a football player's career, but one would think that given all the quantifiable data on a football player (speed, strength, jumping ability, college career stats, etc.), plus all the intensive attention given to draft candidates that it would be fairly easy to predict who will succeed. But according to the Sporting News, less than a third of the 319 supposedly "can't miss" prospects selected in the first round of the last 10 NFL drafts have been selected to even one Pro Bowl—an acclaimed (though admittedly somewhat flawed) measure of football success. Only 17% went to multiple Pro Bowls. (See http://aol.sportingnews.com/nfl/story/2012-04-22/nfl-draft-2012-first-round-disappointments.)

Another Internet site (http://www.advancednflstats.com/2009/04/career-success-by-draft-order.html) shows that Pro Bowl selection *does* correlate with order chosen in the draft, as does years ultimately played as a starter, but these correlations are not nearly as strong as one might expect. Moreover, the authors of the site argue that being chosen high in the draft is something of a self-fulfilling prophecy. Teams spend huge amounts of money on high draft picks and tend to do anything possible to justify the funds spent and the players chosen. Players who are high draft picks tend to get lots of playing time and extra coaching assistance because they are expected to succeed; indeed, it is embarrassing to the team if they do not. Thus, high draft picks have something of an unfair advantage that skews the statistics.

The bottom line: if NFL "hiring" experts—with tens of millions of dollars at stake, who choose from among highly scrutinized candidates for which reams of rigorous data are known, in an endeavor where success is fairly easily measured (winning

games)—can't reliably choose outstanding performers, what chance do you have to pick good employees?

*****

Here's another Human Resources issue that might be of interest to security managers: Baby Boomers were born between 1946 and 1964. Generation X are those that followed the Baby Boomers. Millennials are the generation born between 1982 and 1999. Each generation, it is claimed, has its own characteristics. Millennials supposedly tend to have trouble dealing with conflict and lack the ability to deal effectively with confrontation. Their communication style is quite different from earlier generations. According to Linda Gravett with the HR consulting firm Gravett & Associates, Millennials tend to work more effectively when paired with Baby Boomers than with Gen Xers who are, after all, near the age of their parents and may invoke ingrained parent-child conflicts.

*****

Increasingly, courts, government, and society as a whole are grappling with issues of rights, responsibilities, and liabilities of private security officers. There was an interesting court case here in Illinois recently. In *Poris v. Lake Holiday Property Owner's Association*, the Appellate Court ruled that the private security officers hired by the homeowners association of the Lake Holiday subdivision in LaSalle County, Illinois do not have the legal authority to stop, detain, or inspect the driver's license of persons violating association rules (as opposed to Illinois laws). The court also ruled that the security officers could not use flashing amber lights in the process of making such a stop, but that the use of video recording equipment (if openly reported) and radar to measure vehicle speed was permitted. For more information, see http://www.illinoisrealtor.org/drlegalnews/Mar2012/casestudies.

Update 1/25/2013: The Illinois Supreme Court overturned this lower court ruling on both the stop/detain issue and the flashing lights. The plaintiff, former DuPage County prosecutor, Ken Poris asserted that this new ruling "…is going to have possibly some real serious consequences". For more information, see the *Chicago Tribune*, January 26, 2013, page 4.

*****

The curse of auto spell checkers: In February of this year, a college student in Oakwood, Georgia texted a friend that he would be near the West Hall High School. He meant to text, "Gunna be at West Hall this afternoon." But his smart phone's spell checker changed "Gunna" to "Gunman". Then he sent the text to the wrong phone number. What resulted was a lockdown at the high school and general chaos.

*****

Also, in the news: Officials with Prince George's County in Maryland are having to install security cameras to monitor their speeding cameras. Seems six of the speeding cameras have been burned, vandalized, and shot at by angry motorists. No word yet on when security cameras will be installed to monitor the security cameras monitoring the speeding cameras.

*****

The Vulnerability Assessment Team (VAT) at Argonne National Laboratory hosts and edits the *Journal of Physical Security* as a free, public service. Part of what we get out of it (other than getting to read some really interesting papers about physical security) is a chance to shamelessly plug our own work and views from time to time. Here are some recent news stories about the VAT. (The first two are also very good general reviews on the subject of election security.)

Victoria Collier, "How to Rig an Election", *Harper's Magazine* **325**, 33-41 (November 2012), http://harpers.org/print/?pid=225772

Laura Spadanuta, "Machine Politics", *Security Management* **56**(10) 50-57 (September 2012), http://securitymanagement.com/article/machine-politics-0010437?page=0%2C0

"How Your Vote Can Be Hacked", http://money.cnn.com/video/technology/2012/10/31/ts-voting-machine-hack.cnnmoney/index.html?iid=HP_River

"How Reliable is Electronic Voting in the US Election", BBC Click Radio Program, http://www.bbc.co.uk/programmes/p0104hxr

Wolfgang Stieler, "Wahl Ohne Kontrolle", *Heise Technology Review*, http://www.heise.de/tr/artikel/Wahl-ohne-Kontrolle-1733733.html

RT News live interview, http://www.youtube.com/watch?v=Ksvd7FJtNuU&list=UUczrL-2b-gYK3l4yDld4XlQ&index=5&feature=plcp

Eric Parizo, "Researcher Details Findings on Spoofing GPS, Malicious Insiders", http://searchsecurity.techtarget.com/video/Researcher-details-findings-on-spoofing-GPS-malicious-insiders

Eric Parizo, "Vulnerability Researcher on Layered Security Plan Mistakes", http://searchsecurity.techtarget.com/video/Vulnerability-researcher-on-layered-security-plan-mistakes

*****

As vulnerability assessors, we frequently encounter denial from security managers and bureaucrats about security flaws, or even are the targets of their fear and anger that would more productively be directed at their true adversaries. The latter phenomenon is predicted by **Feynman's Maxim**: An organization will fear and despise loyal vulnerability assessors and others who point out vulnerabilities or suggest security changes more than malicious adversaries.

The name for this maxim comes from the entertaining book, *Surely You are Joking, Mr. Feynman!*, published by W.W. Norton in 1997. During the Manhattan Project, when physicist Richard Feynman pointed out physical security vulnerabilities, he was banned from the facility, rather than having the vulnerability dealt with—which would have been easy. (A total of 120 more security maxims can be found at: http://www.ne.anl.gov/capabilities/vat/seals/maxims.shtml.)

Oliver Burkeman recently published an interesting essay in the *Wall Street Journal* (http://online.wsj.com/article/SB10001424127887324705104578147333270637790.html) that reminds us of the power of negative thinking, specifically the "premeditation of evils".

As Burkeman points out, the ancient Greek and Roman Stoic philosophers advised people to periodically think about the worst thing that could happen as a way of chilling out when facing risks and uncertainties. As modern psychologists know, mentally focusing in detail on the worst that can happen has (somewhat counter-intuitively) an amazing ability to make the future seem a lot less scary to people with fears and anxieties. Interestingly, thinking about the worst that can happen is also a very good security strategy. Thus, by focusing on the negative, you can have better security AND stop freaking out!

Failure to consider the worst that can happen may make you the victim of **Mahbubani's Maxim**: Organizations and security managers who cannot envision security failures, will not be able to avoid them. This maxim is named for scholar and diplomat Kishore Mahbubani. He meant to apply this general principle to politics, diplomacy, and public policy, but it is also applicable to security.

*****

We always try in this journal to introduce fresh approaches to thinking about security. Bad poetry is one possible approach that has been inexplicably ignored by other security journals. So here we offer some bad haiku poetry about security.

English haiku is an English language version of the Japanese haiku poetic tradition of terse, fragmentary poems that paint a verbal picture. Each English haiku poem typically consists of 3 lines of 5, 7, and 5 syllables, respectively. Thus…

**Security fights:**
**evil, denial, conceit.**
**The dismal science.**

**Over-Confidence.**
**Denial. Wishful Thinking.**
**The real enemies.**

**Primitive methods**
**often overcome high-tech.**
**So don't get dazzled!**

**If you're happy with**
**your security. Well, then...**
**so are the bad guys.**

**Tamper Detection**
**is only as good as your**
**Seal Use Protocol!**

**gruntled employees**
**much safer than disgruntled**
**treat everybody well!**

**Insiders attack.**
**Many different reasons.**
**But revenge burns hot.**

-- Roger Johnston
Argonne National Laboratory
December 2012

Viewpoint Paper

# The Japan Earthquake and Tsunami: Their Implications for the U.S.

Paula D. Gordon, Ph.D.

Auburn University Center for Governmental Services and
Eastern Kentucky University College of Justice and Safety,
Department of Safety, Security & Emergency Management

What can be made of the Japanese 9.0 earthquake and tsunami that occurred in March of 2011? What can be made of the assessments of the damage done to date, of ongoing damage to nuclear reactors there, and what are the possible consequences following from that ongoing damage and the implications for the safety of nuclear power plants in the U.S? In addition, what are the implications for nuclear security in the aftermath of an earthquake of devastating proportions beyond the magnitudes that nuclear facilities have been built to withstand?

There are differences in the views of experts making assessments concerning the extent of damage and the consequences of the damage, the potential for continuing damage and the consequences and implications of the damage that can potentially occur as a result of high magnitude earthquakes. There are differing views concerning the implications of the Japan Earthquake for the safety and security of nuclear power plants around the world, particularly those nuclear power plants built in seismically active areas, such as the faults near and along the West Coast of the U.S., in New York near New York City, and the New Madrid fault in the center of the U.S.

No nuclear power plant anywhere in the world appears to have been built to withstand an 8.3 or higher magnitude earthquake. According to Japanese power plant officials, some nuclear power plants in Japan, surprisingly enough, were only built to withstand an 8.2 earthquake at most.[1] Others have quoted lower figures.[2]

Even Los Alamos National Laboratory has shown a concern for seismic safety in planning a Chemistry Metallurgy Research Replacement Facility in Northern New Mexico. That facility in all likelihood will include involvement in nuclear and plutonium research. Current plans are to build a facility that will withstand an earthquake of up to 7.3 magnitude.[3]

According to one source, the nuclear power plants in California, San Onofre and Diablo Canyon, have not been built to withstand earthquakes that exceed 7.0 or 7.5 in magnitude respectively.[4] It is said that the Indian Point power plant which is located on a fault in New York has been built to withstand only a 6.0 magnitude earthquake.[5] (To the author's knowledge no nuclear power plant anywhere in the world has been built to withstand tsunamis generated by 8.3 or higher earthquakes.)

Tsunami threats aside, it is arguable, however, whether or not California nuclear power plants could withstand an earthquake that exceeded a 6.9 magnitude. The reason why these nuclear power plants would be unlikely to withstand an earthquake of this magnitude is owing to the way the plants have been constructed and the failure, according to some cutting edge mechanical engineering researchers, of those who set the standards used in configuring nuclear reactors and building nuclear power plants. According to these mechanical engineering researchers, those setting the standards for bearing clearances in primary fluid coolant pumps and generators and other rotor bearing systems in nuclear reactors have failed

to take fully into account gyroscopic and coriolis effects on moving systems in an earthquake of significant magnitude.[6,7]

In the 1980s and 1990s, a U.S. mechanical engineering research expert, A. H. Soni, whose work had been funded by the National Science Foundation, focused on the seismic analysis of rotor bearing systems, including primary fluid coolant pumps and generators involved in the day-to-day operation of nuclear reactors. His research indicated that while gyroscopic and coriolis effects on such systems were taken into consideration by earthquake engineers in Japan, they were not being taken into consideration by those responsible for setting standards for nuclear reactors in nuclear power plants in the U.S. According to Soni, the reason for this was that the academic and professional backgrounds of Japanese nuclear power plant engineers tended to be far more cross disciplinary than the backgrounds and academic training of the structural engineers in the U.S.[8] This is important in that in the U.S., the standards for nuclear power plants have tended to be set by structural engineers. According to the same source, structural engineers have tended to be at the top of the professional "pecking order" of U.S. engineering professionals and it is the structural engineers who have played the key role in setting power plant standards for nuclear power plants built in seismically sensitive areas in the U.S. As a result of these differences in background and knowledge, the standards for the bearing clearances in rotor bearing systems including primary fluid coolant pumps and generators and other rotor bearing systems in Japanese power plants were mounted differently than those in U.S. power plants. This was done to prevent the likelihood of such pumps and generators and other rotor bearing systems becoming projectiles in an earthquake and damaging the reactor and the facility.

In the 1980s and 1990s, several individuals, including Professor Soni, attempted to raise awareness concerning these matters. He felt that the Nuclear Regulatory Commission (NRC) had not adequately understood these concerns and had not brought adequate attention to them. In an August 7, 1992 letter to this author, Soni summed up the implications of his work and his 1984 article on the seismic analysis of rotor bearing systems as these pertained to nuclear reactors[9] as follows:

> While most of the research is done to advance the fundamental understanding of the system, nothing has been done anywhere in the public domain knowledge to develop standards for the bearing clearances in the primary fluid coolant pump, the generator (..and other systems) that are involved in the day-to-day operation of a nuclear reactor. It is a very serious problem in the maintenance and upkeep of a reactor power plant. During seismic activities, this pump may have a breakdown and possible leak of the radioactive primary fluid. Such things may even happen during normal operation when proper maintenance procedures are not (followed). Hence, the problem is of a very serious nature…[10]

Soni gave briefings and spoke with individuals in major roles of responsibility in government. Other individuals shared the implications of Soni's research with others in government and industry in the U.S. These efforts apparently had little or no success in raising awareness. NRC officials as well as U.S. industry officials were not open to considering the work or the implications of the work done by Professor Soni. In fact, some NRC officials in the research development branch had expressed the view to this author that the Professor was likely an intervener.[11] In fact, the Professor had no political agenda whatsoever.[12]

The climate today seems only slightly more hospitable for ongoing efforts to raise awareness of these concerns for the safety of nuclear reactors and nuclear power plants in seismically sensitive areas in the U.S. The Japan Earthquake and Tsunami that have triggered the Fukushima nuclear power plant disaster have opened the eyes of many concerning comparable risks and vulnerabilities in the U.S. Owing to the scientific and technological complexities surrounding nuclear power plants and nuclear power plant safety, many of those in positions of responsibility in government and industry have turned to experts whom they assume understand these complexities. The following questions arise:

> What is the basis of the understanding of these experts?
>
> Are these experts equally knowledgeable concerning both structural and mechanical engineering principles?
>
> Do they recognize that those setting the standards for the building and configuration of nuclear reactors in nuclear power plants in seismically sensitive areas in the U.S. have not tended to take into consideration seismic analysis of rotor bearing systems and mechanical engineering principles?
>
> Do they know that there are questions concerning whether or not nuclear power plants in the U.S. can withstand earthquakes of the magnitudes that structural engineers have assumed were sufficient?

There are disasters such as the Challenger Disaster, the Kansas City Hyatt walkway collapse and the Minneapolis bridge collapse where after action reports and assessments were done to try to determine the exact reasons for the failures. Experts from various relevant disciplines

were convened. The conclusions reached by those voicing a "majority opinion" in the reports have sometimes overshadowed or even drowned out a "minority" viewpoint. In the case of the Challenger Disaster Commission deliberations, Richard Feynman, the renowned physicist, a minority of one, provided a simple explanation of the causes of failure: the failure of the O-rings owing to the frigid temperatures at the time of the launch. His assessment echoed Roger Bojoly's pre-launch warnings. Bojoly was an engineer who had vehemently warned against launching in cold conditions owing to the likely failure of the O-rings.

Professor Soni who passed away several years ago was like both Roger Bojoly and Richard Feynman with respect to their prescience and perspicacity. Warnings implicit as well as explicit in his government-funded research that should have been listened to and acted upon apparently have not been heard. One hopes that all those with responsibilities for the safety of nuclear power plants as well as other nuclear facilities will call on a wider circle of experts when determining risks and vulnerabilities and that such circles of experts will be facilitated by generalists who are not closed-minded or untutored when it comes to the pertinence of all relevant and essential areas of expertise. In the case of the safety and security of nuclear power plants, this would include the expertise of those on the cutting edge of mechanical engineering.

If it is indeed the case that there is no certainty at present that nuclear power plants built in seismically sensitive areas in the United States will even be able to withstand the magnitude of earthquake they were built to withstand, nuclear safety and nuclear security and, hence, public safety are at far greater risk than most individuals have imagined or presently imagine. Given the possibility of worst case scenarios such as the events that occurred and continue to unfold in Fukushima and given the possibility of higher, presently unplanned for, magnitudes

of earthquakes that could occur in the U.S., matters involving nuclear power plant safety and security surely need to be more seriously reviewed and rigorously reconsidered than is presently the case and actions need to follow to prevent similar worst case scenarios from occurring here.

**About the Author**

Dr. Gordon is an educator, researcher, writer, and consultant. Her specialty areas include emergency management and homeland security. Her websites can be found at http://GordonHomeland.com and http://GordonPublicAdministration.com. She is currently teaching courses on homeland security and emergency management-related topics for several universities.

Earthquakes have been one of her particular interests. During the time she worked for U.S. Federal Emergency Management Agency and the U.S. Environmental Protection Agency, she became particularly interested in nuclear power plant vulnerability to earthquakes. As a result of her previous association with the Research Applied to National Needs Program of the National Science Foundation (NSF), she had heard a presentation by A. H. Soni, a mechanical engineering researcher whose research had received funding from NSF's Earthquake Engineering Division. His research focused in part on the seismic analysis of rotor bearing systems, including primary fluid coolant pumps and generators involved in the day-to-day operation of nuclear reactors. He was particularly concerned with the standards for bearing clearances on systems that are likely to be significantly impacted by seismic activity.

On becoming informed regarding Soni's work, the author expanded her interest and over the years has had discussions concerning the implications of Soni's research with individuals at the Nuclear Regulatory Commission as well as with individuals from other places in government, academia, non-governmental organizations, and the nuclear power industry. The vulnerabilities of nuclear reactors in the U.S., according to Soni, were not well understood by those setting the standards for nuclear reactors in the U.S. Those standards were in his view typically set by structural engineers rather than by mechanical engineers who had an understanding of seismic impacts on rotor bearing systems.

Based on her understanding of the work of Soni and his colleagues, the author concludes that there is no certainty at present that nuclear power plants built in seismically sensitive areas in the United States will be able to withstand the magnitude of earthquake they were built to withstand, and that nuclear safety and nuclear security and hence public safety are at far greater risk than most individuals have imagined or presently imagine.

E-mail: pgordon@starpower.net

## References

[1] Jacob Goodwin (2011 March 13) "Nuke plant owner in Japan didn't plan for an 8.9 magnitude earthquake," GSNMagazine.com. Retrieved August 15, 2012 at http://www.gsnmagazine.com/node/22680?c=disaster_preparedness_emergency_response .

[2] Yuka Hayashi and Mari Iwata (2011, March 13) "Japan Struggles to Control Reactors." WSJ.com. Retrieved August 15, 2012 at http://online.wsj.com/article/SB10001424052748703555404576195700301455480.html .

[3] Jeri Clausing (2011 December 18) "Quake risk eyed amid concerns about planned N.M. nuclear lab," **Washington Post**, p. A7 .

[4] Travis Madsen (2011 March 14 as updated March 16) Frontier Group.org. Retrieved August 16, 2012 at http://www.frontiergroup.org/blog/blog/how-large-of-an-earthquake-could-u.s.-plants-withstand. The following material is quoted verbatim:

According to the U.S. Nuclear Regulatory Commission, historical earthquake activity at the location of a proposed plant is an important part of reactor design standards. Commission staff determine the largest "credible" earthquake that could occur at a given site, and require engineers to design the plant to withstand that force, plus an added margin of safety.

- According to a spokesperson for Southern California Edison, the San Onofre nuclear power plant is designed to withstand a magnitude 7.0 earthquake happening 5 miles away.
- According to the Nuclear Regulatory Commission, Diablo Canyon is designed to withstand a magnitude 7.5 earthquake 3 miles away.
- A spokesperson for the Indian Point nuclear power plant in New York told Reuters that the plant was designed to survive an earthquake of magnitude 6.1 on the Richter scale.

See also: Nuclear Regulatory Commission (May 2011 Reviewed/Updated *2012 May 29)* Fact Sheet on Seismic Issues for Nuclear Power Plants. Retrieved August 15, 2012 at http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/fs-seismic-issues.html .

[5] Ibid.

[6] V. Srinivasan and A.H. Soni, "Seismic Analysis of a Rotor-Bearing System," **Earthquake Engineering and Structural Dynamics**, Vol. 12, 287-311 (1984) L.E. Suarez, M.P. Singh, and M.S. Rohanimanesh (1992), Seismic response of rotating machines. **Earthquake Engineering & Structural Dynamics**, 21: 21–36, doi: 10.1002/eqe.4290210102. For abstract see http://onlinelibrary.wiley.com/doi/10.1002/eqe.4290210102/abstract. Abstract retrieved August 15, 2012. A quote from the abstract: "The rotational input terms in the forcing function, however, are quite important and can be ignored only when they are not very strong."

[7] L.E. Suarez, M.P. Singh, and M.S. Rohanimanesh (1992), Seismic response of rotating machines. **Earthquake Engineering & Structural Dynamics**, 21: 21–36, doi: 10.1002/eqe.4290210102. For abstract see http://onlinelibrary.wiley.com/doi/10.1002/eqe.4290210102/abstract. Abstract retrieved August 15, 2012. A quote from the abstract: "The rotational input terms in the forcing function, however, are quite important and can be ignored only when they are not very strong."

[8] A.H. Soni, personal communication, 1984.

[9] V. Srinivasan and A.H. Soni, ibid.

[10] A.H. Soni, personal communication, August 7, 1992.

[11] Personal communication with an individual in the research development branch at NRC, February 8 1993 and separately reported in a personal communication with A. H. Soni, November 1992.

[12] A.H. Soni, personal communication, November 1992.

Journal of Physical Security 6(1), 10-21 (2012)

# Lock Opening by Bumping: Physical Analysis and Secure Lock Designs

Alexei Toropov, Ph.D.
Dierre Spa, Italy
tel: +393476701025, e-mail: alexei.toropov.dierre@gmail.com

**Abstract**

There are various techniques for defeating locks based on exploiting vibration. In recent years, one of these techniques for manipulating cylinder locks, called "bumping", has become widespread. The problem is that a large variety of mechanical locks can be opened quickly, in a non-destructive manner by using simple attack tools. We studied the physical phenomena responsible for the vibration techniques of lock opening. We considered the period of time during which the pins of a cylinder lock remain separated as a function of natural frequency, damping properties, and lock design parameters. On the basis of this analysis, we suggest some changes to lock design and assembly that can enhance the security of the lock and resist bumping attacks.

**Key words:** locks, security lock, lock picking, bumping, design of secure locks

## Pin Tumbler Cylinder

When people talk about "the cylinder lock " or “the pin tumbler cylinder”, they have in mind the classic locking mechanism invented by Linus Yale in 1861. The concept is so simple and effective that it remains the basic design principle of modern locks. The mechanism essentially consists of two main parts: the housing and cylindrical plug with axial keyway. See figure 1. A number of holes have been drilled up to the keyway in the transverse direction through the housing and the plug. In each hole, there is placed a key pin, a driver pin, and a compression spring. When the proper key is inserted in the keyway, each cut on the key has the correct depth which allows a coincidence between the shear lines of the key pins and driver pins, and the shear line of the housing and plug. When this occurs, the plug can be turned and the lock unlocked. If, on the other hand, the corresponding depth of the cut on the key differs from the correct value (either too high or low), the cylinder will not rotate.

If we assume that the number of different depths varies from 6 to 9, and that the number of the pin pairs is equal to 6 (which is typical for many standard cylinder locks), then the number of possible code combinations can approach half a million. Such a large value means that, despite being enclosed in relatively limited dimensions, the Yale mechanism provides significant levels of key uniqueness and security.

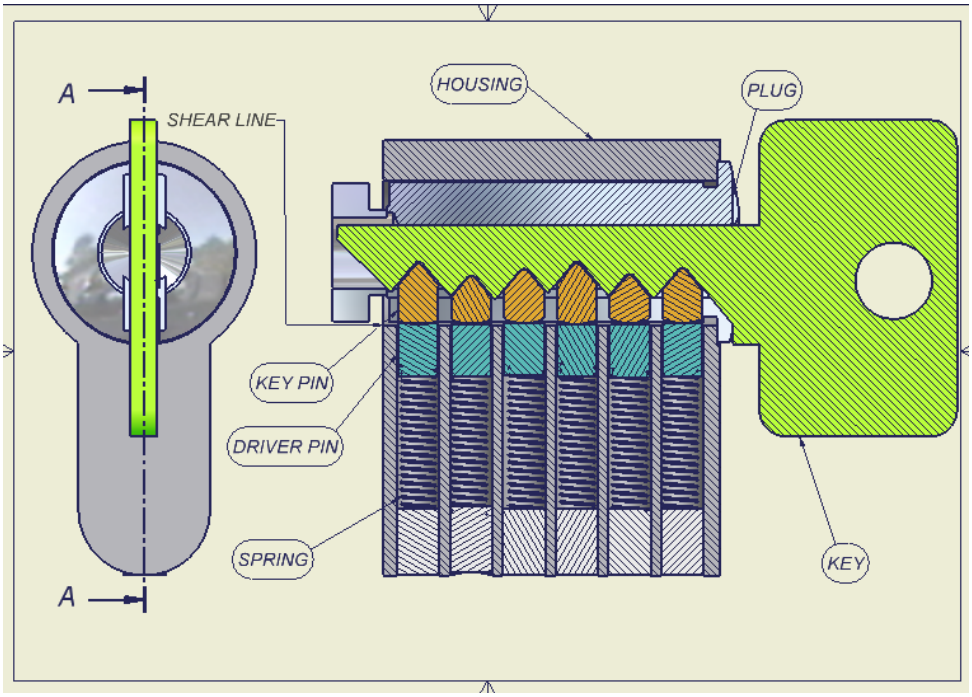



Figure 1 - The pin tumbler cylinder.

In recent years, however, it has become widely recognized that all cylinders which employ this classic Yale design are at risk due to the simple and easily applicable techniques based on the movement of the pins due to the impact or vibration applied to the lock in different ways. These can include the use of picking guns such as the "snapper pick"[1], through more sophisticated attack tools utilizing electric motors. All these attack techniques rely on the fact that the key pin and driver pin can be separated for a brief instant of time. During this small period of time, the skilled operator attempts to turn the plug of the cylinder.

One of the most successful of such vibration attack methods is "bumping", described in detail elsewhere.[1,2] In contrast to other vibration methods, bumping allows the simultaneous, synchronized movement of the pins. Bumping requires use of a bump key. This is a key which can be inserted into the keyway, and that has all cuts at every position at the maximum possible depth. In addition, the tip and the shoulder of the key must be milled for some fractions of a millimeter. If this bump key, once inserted, is hit by some impact tool, it transfers energy to the first pin of the lock. The first pin then transfers the energy to the second pin, which moves away from the first one, until the spring causes it to rebound back.[2] This approach allows the major types of pin tumbler cylinders to be opened quickly, without damage, through the use of simple tools.

The bumping technique has been investigated previously from the theoretical point of view [1,2] but only one part of the whole system of elements was considered, namely the kinematic behavior of the key pins and driver pins during purely elastic impact.

**The Behavior of Cylinder Parts During Bumping**

The tools used for bumping are shown in figure 2. The schematic model for bumping is depicted in figure 3, where $M_h$ and $V_h$ are the mass and velocity of the bump hammer, respectively, and $M_k$ and $V_k$ are the mass and velocity of the bump key. The values of velocities correspond to the values after impact.

For this model, we assume that the impact between all parts is purely elastic, and that they move without friction. This approximation is close to realty for low initial displacements just after the parts collision.

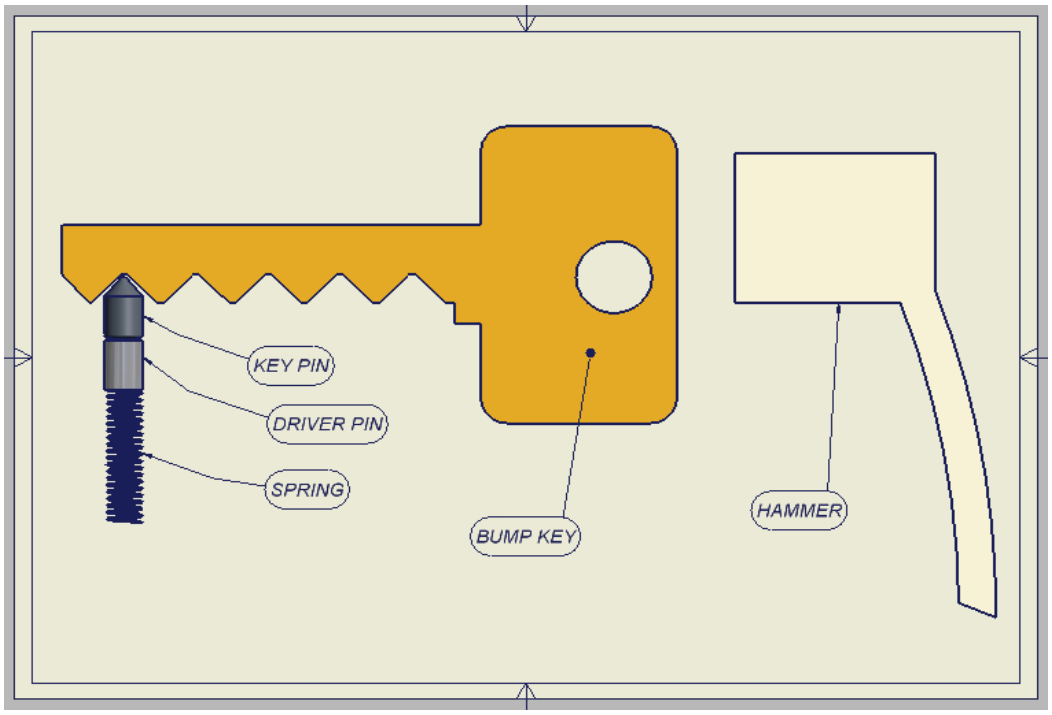



Figure 2 - Bumping components.

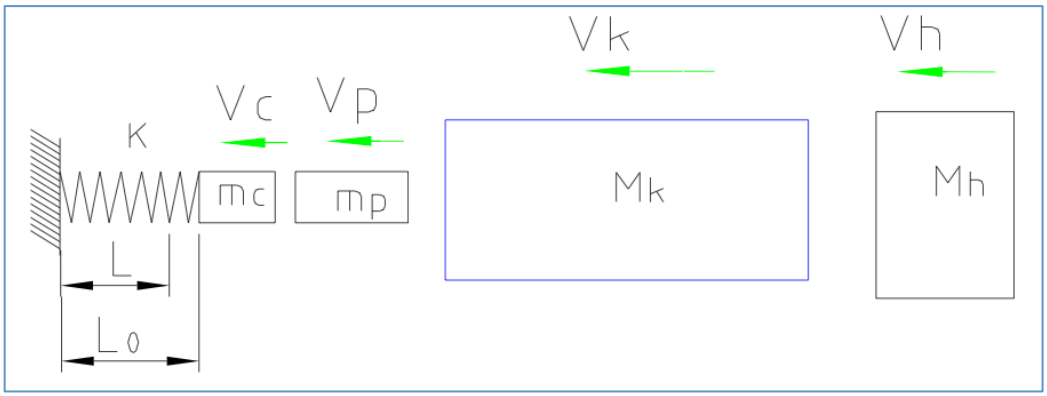



Figure 3 - Model representation of the bumping process.

The bumping procedure initiates with striking of the bump key with the hammer. If the hammer's initial velocity is $V_0$, the subsequent behavior of the hammer and bump key can be described by applying the following physical laws:

$$M_h \cdot \overline{V}_0 = M_h \cdot \overline{V_h} + M_k \cdot \overline{V_k} \qquad \text{the law of conservation of momentum} \qquad (1)$$

$$\frac{M_h \cdot V_0^2}{2} = \frac{M_h \cdot V_h^2}{2} + \frac{M_k \cdot V_k^2}{2} \qquad \text{the law of conservation of energy} \qquad (2)$$

In equation (1) we assume one-dimensional displacement of the parts before and after the collision, therefore the vector values of momentum can be substituted with their scalar values.

From (1) and (2) we can obtain the velocity of the bump key after collision:

$$V_k = \frac{2 \cdot V_0}{\frac{M_k}{M_h} + 1} \qquad (3)$$

Equation (3) leads to the interesting conclusion that the velocity of the key after impact does not differ significantly from the velocity of the hammer before impact, even if the mass of the hammer is considerably greater than the key mass. In fact, in the upper limit case where the ratio $M_k/M_h \rightarrow 0$, the key has only twice the hammer velocity, and when $M_k \sim M_h$, we have $V_k \sim V_0$. Thus, for purely elastic impact, the mass of the hammer has little importance (over a reasonable mass range) for successfully opening the lock with bumping. Probably more critical is the handiness and convenience of manipulation.

The same approach can be apply to estimate the velocity of the key pin. We assume that a purely elastic collision occurs between the key and the pins. In this case, equation (1) becomes:

$$M_k \cdot V_k = q \cdot m_p \cdot V_p + M_k \cdot V_{1k}$$

The vector values of velocity have been substituted with their scalar values. But due to the changing of the pin movement direction, we insert the coefficient $q$, which depends on the angle between the direction of key movement and the plane of collision with the key pin. This coefficient is equal to 1 for a frontal ($\pi/2$) collision, whereas $q < 1$ for angles of collision less then $\pi/2$. For real keys, we assume that this angle ranges between $\pi/2$ and $\pi/4$, and $q$ is bounded by $\frac{1}{2} < q < 1$. Combining this equation with the energy conservation equation, we find the initial velocity of the key pins just after impact:

$$V_p = \frac{2qV_k}{\frac{q^2 \cdot n \cdot m_p}{M_k} + 1} \quad (4)$$

where n is the number of pins in the cylinder, usually equal to 6 or 7. Others terms are shown in figure 3.

We assume that the mass of the pins is significantly less than the mass of the key. This is reasonable because typical dimensions for the driver pins are ø3 x 5 mm, corresponding to about 0.3 grams (for brass), whereas the mass of the key is around 15 - 25 grams. Thus, $q^2 \cdot n \cdot m_p << M_k$, and taking into consideration that $V_k \approx V_0$ for the majority of situations, the pin velocities can be estimated to be:

$$V_c \approx V_p \approx \gamma \cdot V_0 \quad (5)$$

where $1 < \gamma < 2$. Here we have made the reasonable assumption that the velocity of the key pin is nearly equal to velocity of the driver pin, due to the elastic collision between them and their nearly identical mass values, along with their same direction of movement. Hence, we can conclude that the initial velocity of the driver pins during a bumping attack doesn't differ significantly from the velocity of the hammer.

Obviously, for bumping attacks the following rule is valid: the longer the time period when two pins (key pin and driver pin) are separated, the more likely the bumping will succeed. Therefore, it is useful to estimate this period of time, and identify the most important parameters responsible for the changing of this value.

Because the mass of the driver pin is the same order of magnitude as the key pin, the velocity of the driver pin after impact is approximately equal to $V_p$. The kinematic behavior of the driver pin after impact can be precisely described by the force balance equation, well known in the form of the differential equation for a harmonic oscillator [3, 4], without taking into consideration the gravitational force:

$$m_c \cdot \frac{d^2x}{dt^2} + c \cdot \frac{dx}{dt} + k \cdot x = -F_0 \quad (6)$$

where *x* is the displacement of the pin from the initial position, dx/dt and $d^2x/dt^2$ are the velocity and acceleration of the driver pin, respectively, *c* is the friction coefficient, and *k* is the spring stiffness (or spring constant). The sum of the forces in the left part of the equation (6) are set equal to the force $F_0$ caused by the spring, when mounted into the cylinder with some initial compression deformation.

The damping ratio $\varsigma^2 = \frac{c^2}{4 \cdot k \cdot m_c}$ critically determines the behavior of this system.

There are three clearly distinguished kinematic behaviors of the system:

1. The undamped situation (no friction) where $c^2 << 4\ k\ m_c$

2. The damped situation. This occurs when the friction forces are sufficiently strong to change the kinematic behavior of the key pins and driver pins, but at the same time, the pins can still move without much resistance: $c^2 \leq 4\ k\ m_c$

3. The over damping situation when the friction force significantly obstructs the moving of the pins. This case has no practical relevance for bumping a pin tumbler cylinder because with over damping, the pins can barely move and the cylinder won't operate properly.

**Undamped Situation**

In this case, equation (6) reduces to

$$m_c \cdot \frac{d^2x}{dt^2} + k \cdot x = -F_0 \qquad (7)$$

If we substitute the variable $y = x + \frac{F_0}{k} = x + \Delta L$, where

$$\Delta L = L_0 - L \qquad (8)$$

is the difference between the free ($L_0$) and mounted ($L$) lengths of the spring (see figure 3), we can rewrite (7) as follows:

$$m_c \cdot \frac{d^2y}{dt^2} + k \cdot y = 0$$

which has the well known solution $y = A\sin(\omega_0 \cdot t + \phi)$, where A and $\varphi$ are the amplitude and phase of oscillation, which depend upon initial conditions of the pin, and where $\omega_0 = \sqrt{\frac{k}{m_c}}$ is the natural angular frequency of oscillation.

Substituting for $y$, we obtain: $x = A\sin(\omega_0 \cdot t + \varphi) - \Delta L$

Based on the initial conditions at t = 0, we have x = 0 and $dx/dt = V_c$ at the start of motion of the driver pin just after impact, and at $t = t_{max}$, we have $x = A - \Delta L$ and $dx/dt = 0$ at the point of maximum distance of the driver pin from the key pin. Given that the period of separation of two pins is twice the time to arrive up to the point of maximum deflection, we have finally:

$$\tau = 2t_{\max} = \frac{1}{\omega}\left[\pi - 2 \cdot \arcsin\left(\frac{V_c^2}{{\omega_0}^2 \cdot \Delta L^2} + 1\right)^{-1/2}\right] \quad (9)$$

This expression gives the exact solution of the time interval at which two pins are separated. It should be noted that for all real designs of a pin tumbler cylinder, the following condition will be always satisfied:

$$\frac{V_c^2}{{\omega_0}^2 \cdot \Delta L^2} = \frac{m_c \cdot V_c^2}{k \cdot \Delta L^2} >> 1$$

This is due to the fact that the velocity of the driver pin after impact is around a meter per second, but the distance of the spring pre-compression in the mounted state (8) can't be greater than a few millimeters. So, for a reasonable range of pin mass and spring stiffness, the above parameter is much larger than 1. As a result, the expression (9) can be rewritten in the simpler form:

$$\tau = \pi \cdot \sqrt{\frac{m_c}{k}} - 2 \cdot \frac{\Delta L}{V_c} \quad (10)$$

Equation (10) leads to some qualitative conclusions regarding resistance to bumping of pin tumbler cylinder locks in the undamped state. As can be seen, by increasing the stiffness of the spring ($k$) and the distance of pre-compression of the spring in the mounted state, along with decreasing the mass of the driver pins, it is possible to improve the bumping resistance due to the fact that the time, $\tau$, diminishes. In order to do some quantitative estimations, we will considered realistic locks, but to cover a whole range of different designs, we take into consideration 2 extremes cases: one with a very high spring stiffness and extremely low pin mass, along with the maximum possible pre-compression deformation of the spring; and a second case with a very soft spring, maximum mass for the pins, and low pre-compression deformation of the spring.

"Soft" Design

Figure 4 shows various parameters for the lock components, based on a realistic design for a pin tumbler cylinder. The driver pin dimensions are ø3x5 mm. We will assume the spring is made of phosphor bronze, as is often used in real locks due to its high corrosion resistance and good performance, but this kind of spring coupled with pins made from brass can result in an increased susceptibility to bumping. Using the physical characteristics, shown in figure 4, we can calculate the value of spring stiffness and the natural frequency as $k = 29\,{}^{N}\!/_{M}$ and $\nu = \frac{\omega_0}{2 \cdot \pi} = 49 Hz$, respectively.

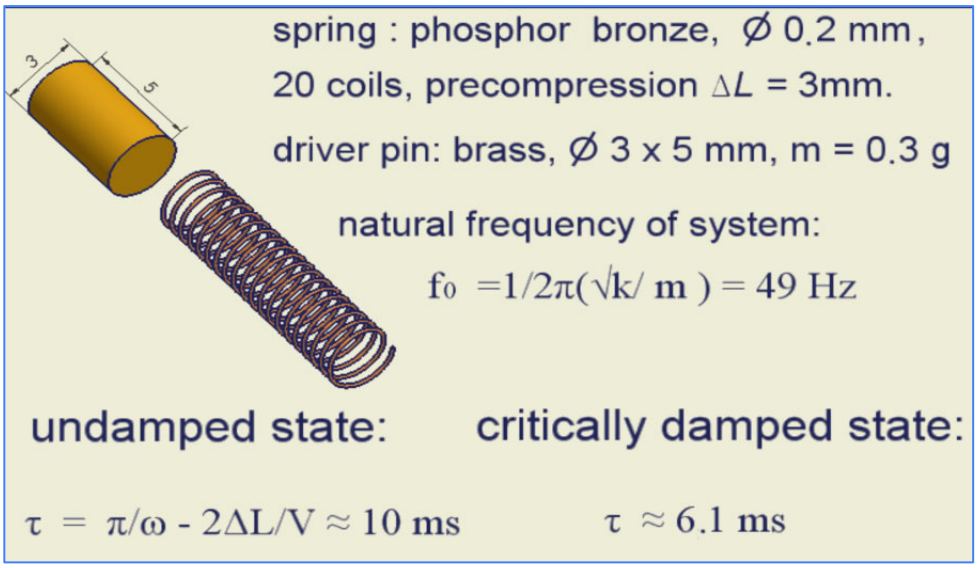



Figure 4 - Design parameters for a "soft" locking mechanism.

The average velocity of the bump hammer can be varied in the range of 6 to 10 meters per second. Taking into consideration that velocity of the pin is approximately the velocity of the hammer (5), we presume in our estimate that $V_c \approx 15\,{}^{M}\!/_{\sec}$. Thus from equation (10) we can obtain the time interval for when the key pin remains separated from the driver pin, before the spring rebounds it back. During this interval of time, the lock cylinder can be turned without the presence of the correct key. It can be seen that this interval is equal to 10 milliseconds for the undamped situation. Due to the fact that an actual lock with the design shown in figure 4 can easily be opened by bumping, we can suppose that a value around 10 milliseconds puts a lock at risk.

"Rigid" Design

This situation suggests some useful countermeasures without making major modifications to the lock. It is necessary to substitute only two elements without changing geometrical dimensions, as shown in figure 5. The brass driver pin used for figure 4 can be replaced with a stainless steel one which has a central hole, in order to significantly decrease the mass (from 0.3 to 0.1 g). The second element to be modified is the spring, now made from stainless steel using a wire with a greater cross section. This increases the spring stiffness to k = 140 N/m.

As a result of these 2 changes, the time period when the pins are separated is equal to only 1.9 milliseconds. Taking into consideration that a real lock designed as described in figure 5 is very difficult to bump, we presume that a value of 1 to 2 milliseconds is near some threshold value for easy opening via the bumping technique. This value seems to be a plausible because a reaction time under 1 millisecond is challenging for most people. It should be noted that in order to make more precise evaluations of the threshold value, it is necessary to obtain more experimental data.

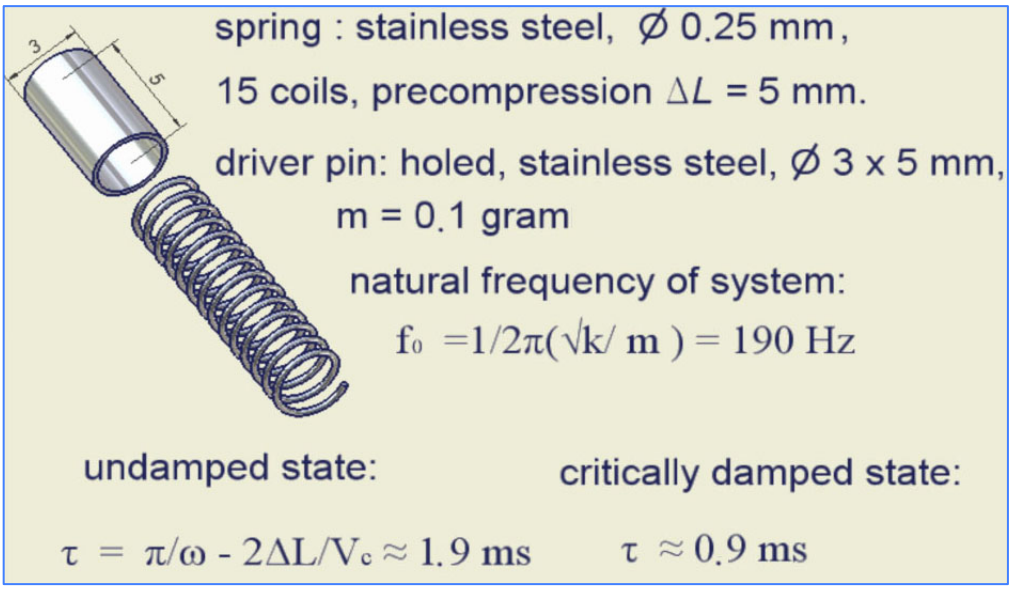



Figure 5 - Design parameters for a "rigid" locking mechanism.

**Damped Situation.**

In any event, a more realistic scenario is the damped situation. This is because a real lock accumulates dirt, dust, pollen, particles, oil, etc. so real locks will never be found in the pure, undamped situation. Equation (6) in this case has the general solution, obtained from equation [4] using $y = x + \Delta L$ which is:

$$x(t) = A \cdot e^{-\varsigma\omega_0 t} \sin(\omega_1 \cdot t + \varphi) - \Delta L \qquad (11)$$

where $\omega_1 = \omega_0 \cdot \sqrt{1-\varsigma^2}$ is the angular frequency of the damped system.

Using the same initial conditions as those used to find expression (9), and assuming $\frac{V_c^2}{\omega_0^2 \cdot \Delta L^2} >> 1$, which is the case for real locks, the time period for which the key pin and drive pin remain separated is:

$$\tau \cong \frac{2}{\omega_1} arctg \frac{\sqrt{1-\varsigma^2}}{\varsigma} - 2 \cdot \frac{\Delta L}{V_c} \qquad (12)$$

As can be seen, equation (12) for the damped situation becomes equation (10) for the undamped situation when the damping ratio $\varsigma \to 0$. On the other hand, the time interval ($\tau$) exponentially descends to the critically damped value at $\varsigma \to 1$ where

$$\tau \cong \frac{2}{\omega_0} - 2 \cdot \frac{\Delta L}{V_c}$$

Figure 6 shows the behavior of the time interval, $\tau$, with increasing damping ratio. The dashed orange line near the solid line indicates the threshold value.

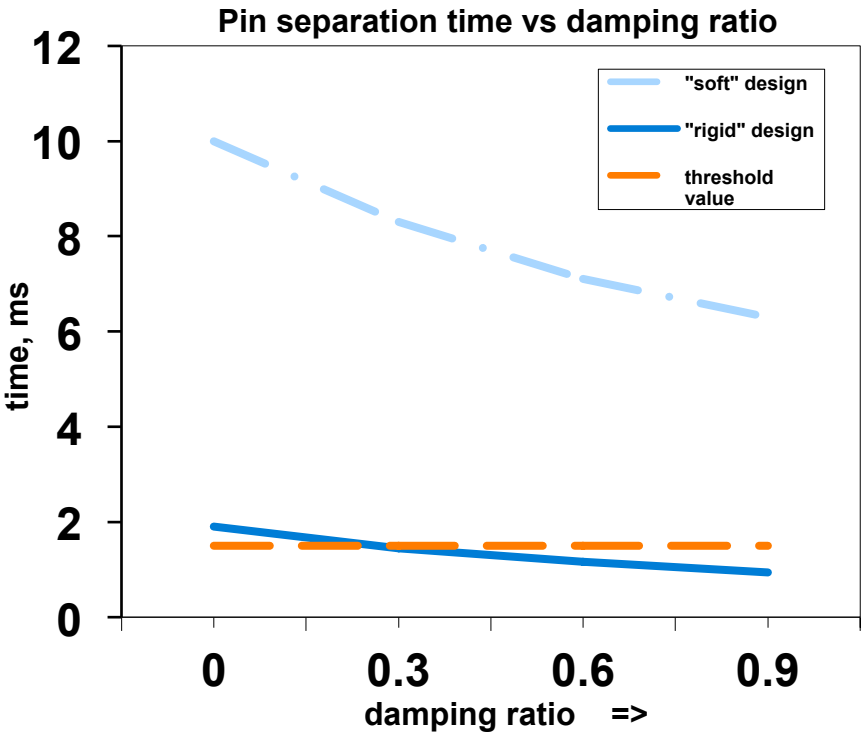



Figure 6 - A graph of the pin separation time, τ, as a function of damping ratio, ζ.

**Discussion**

Important practical conclusions can be made from the graph in figure 6. First, with the passing of time, the resistance to bumping of the cylinder can only improve due to the inevitable accumulation of different types of dirt and contamination, which increases the damping ratio. Second, if an attacker sprays into the cylinder some substance like dense oil, in order to try enhance the possibility of opening by bumping, he is making a mistake. This action increases the resistance to bumping, as shown in figure 6. Moreover, it can be noted that the most effective results for opening the cylinders by any vibration technique (including bumping) will be achieved when the lock is very clean.

The graph in the figure 7 shows the behavior of the pin separation time with increasing natural frequency of oscillation of the spring/driver pin system.

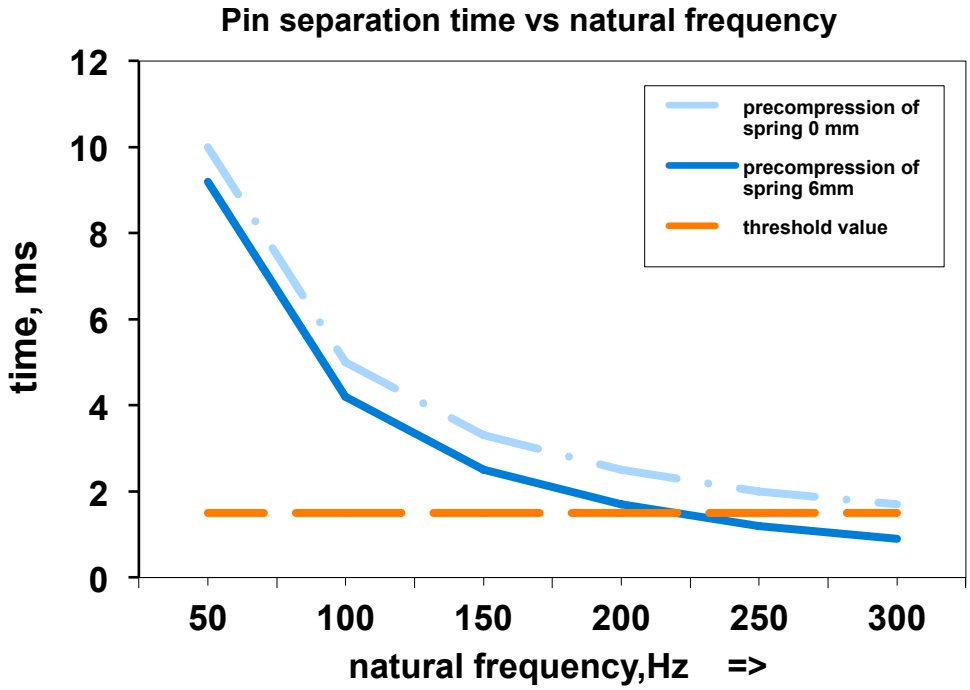



Figure 7 - Pin separation time interval, $\tau$, vs. natural frequency, $f_0 = \omega_0/2\pi$.

It can be seen that the pin separation time decreases hyperbolically with an increasing stiffness-to-mass ratio. So called "soft" mechanisms, which have a natural frequency of oscillation less than approximately 200 Hz, are at risk of being easily opened with bumping.

Note that the value of the spring pre-compression, $\Delta L$, has a relatively low influence on the pin separation time, which is also the case for the velocity of the pins (and hammer). Various locking mechanisms can be evaluated from this point of view. For example, the "radial system" employed by KABA and other manufacturers uses very small pins due to the limited space available in non-vertical directions. These locks, even with a medium range of spring stiffness, result in large natural frequencies. As a consequence, this type of lock is very difficult to bump.

In contrast, mechanisms used by some expensive locks constructed in classic Yale manner, such as the DOM 5-pin, Pfaffenhain, Corbin 5-pin, Zeiss IKON 5-pin and others, have relatively heavy pins. They use springs with low to medium stiffness, and can be easily opened, as has been shown by Barry Wels and Rop Gonggrijp [1]. Evidently the stiffness of the spring cannot be increased infinitely because at high values, the key won't enter the cylinder. The value of stiffness at about *200 N/m* can be considered as the maximum allowable for exploitation reasons. Therefore, to enhance bumping resistance, it is possible to act on both elements: the spring and the driver pin. The mass of the driver pin can be decreased in various ways: by decreasing its external dimensions, by drilling a hole (as shown in figure 5), or by using low density materials. Equation (10) can be used to estimate the bumping (or other vibration attack) risk for each kind of cylinder. All input parameters of this expression can be easily

measured, and reasonable values for the driver pin velocity can be assumed. See the discussion around equation (5).

In the beginning of the discussion, the assumption was made that the masses of the key pins and driver pins are similar, and as a consequence, the velocity of the driver pin is equal to the velocity of the key pin. But sometimes these masses are significantly different, and this fact must be considered in the analysis. Suppose, as above, that a purely elastic collision occurs between the key pin and driver pin. Then, using conservation of momentum and energy before and after the collision (see equations (1) and (2)), we can obtain the precise relationship between the velocity of the driver pin ($V_c$) and key pin ($V_p$): $V_c=2V_p/(1+m_p/m_c)$. Finally, the driver pin velocity can be expressed by means of the velocity of the hammer $V_0$ (a value which can be easily measured). Thus, combining this equation with (10) and (5), we can obtain the expression for a more complete estimation of bumping risk:

$$\tau = \pi\sqrt{\frac{m_c}{k}} - \frac{\Delta L}{\gamma \cdot V_0}(1+\frac{m_p}{m_c})$$

Another important parameter of the cylinder lock is the natural frequency of oscillation. The maximum value at which the cylinder can be operated more or less normally (we presume at about *200 sec$^{-1}$*) can be estimated more precisely by collecting experimental data. Moreover, the value of the natural frequency can also be used as a quantitative parameter for judging a lock's resistance to bumping, and could be included in the standards such as EN 1303 for cylinder locks.

**Acknowledgements**

I would like to express my gratitude to the anonymous reviewers who helped with suggestions, editing, and improving the English. A very special thanks goes to the editor for assistance with editing, corrections, and clarifying the principal results of the paper.

**References**

1. Burry Wels & Rop Gonggrijp, *Bumping locks*, Toool – The Open Organization Of Lockpickers. *http: //www.toool.nl/bumping.pdf* - January 26,2005

2. Marc Weber Tobias, *A Technical Analysis of Bumping*, - Investigative Low Offices, *http://*www.security.org - April, 4, 2006.

3. Harmonic oscillator, *http//en.wikipedia.org/wiki/Harmonic_oscillator*.

4. Serway, Raymond A.; Jewet, John W. (2003), *Physics for Scientists and Engineers*. Brooks/Cole. ISBN 0-534-40842-7.

# How to Choose and Use Seals*

Roger G. Johnston, Ph.D., CPP and Jon S. Warner, Ph.D.
Vulnerability Assessment Team
Argonne National Laboratory

## Introduction

Tamper-indicating seals have been in use for well over 7,000 years.[1,2] Today, seals are widely used for a variety of applications including cargo security, nuclear safeguards, counter-intelligence, theft detection, loss prevention, records security, employee drug testing, and election integrity.[3-11] They protect money, transportainers, footlockers, courier bags, filing cabinets, utility meters, hazardous materials, instrument calibrations, drugs, weapons, computer media, warehoused goods, and other critical items. Despite their antiquity and widespread modern use, there remain quite a few misconceptions, poor practices, and misleading terminology when it comes to seals and seal use.[12-16] This article is a brief primer on how to choose and use seals, and is based on two decades of research by the Vulnerability Assessment Team at Argonne National Laboratory.[17-22]

It's important first off to be clear on what a seal is and what it is not. (See figure 1 for an example of seals.) Unlike a lock, a seal is not intended to delay or discourage unauthorized entry (except possibly in some vague psychological sense). Instead, a seal is meant to leave behind unambiguous, non-erasable evidence of unauthorized access. Complicating the issue is the fact that there are "barrier" seals—devices that are part lock and part seal. Barrier seals have their uses, but the downside is that they cause a lot of confusion in users, and the devices tend to be a compromise, being neither the optimal lock nor the optimal seal for a given application.

Barrier seals are sometimes misleadingly called "security seals" or even "high security seals" in contrast to "indicative seals", but this is sloppy terminology. (All seals have a role to play in security, and "high security" is a value judgment, not a product attribute!) Other terminology to avoid include "tamper-proof seal" and "tamper-resistant" seal. There is no such thing as a seal that cannot be spoofed, and the idea of "tamper resistance" applies more properly to locks, not seals.

Unlike a lock, cutting a seal off a container is not defeating it because the fact that the seal is damaged or missing will be noted at the time of inspection. "Defeating" or "spoofing" a seal means to open the seal, then reseal the container it is used on, but without being detected by the inspection process in use.[18-22] "Attacking" a seal means undertaking a sequence of actions intended to try to defeat the seal.

Seal manufacturers, vendors, and users typically over-estimate the difficulty of defeating their seals. There are at least 105 different generic methods for potentially defeating a seal.[23] These include, for example, picking the seal open without leaving evidence,

*Editor's Note: This paper was not peer reviewed. It originally appeared in *Army Sustainment* ***44****(4), 54-58 (2012).*

counterfeiting the seal, replicating the seal at the factory, changing the serial number, tampering with the database of seal serial numbers, drilling into the seal to allow interior manipulation then repairing the hole, cutting the seal and repairing the damage, not installing the correct seal in the first place (then later replacing it with the correct seal), etc. Full counterfeiting is usually not the most likely attack on a seal unless perhaps the adversary is attacking a large number of seals, or has very limited access time at the seal and its container.

A fundamental fact about tamper detection is that a seal is no better than its "seal use protocol".[1-6,10-12,18] This is the official and unofficial procedures for seal procurement, shipping, storage, check out, installation, inspection, training, reporting, disposal, securing the seal data (such as the recorded seal serial numbers), and securing the seal reader, if there is one. (Typically, 15 seconds of access to either the seal database or the seal reader allows an adversary to defeat 1 or many seals in one quick effort.) Modest seals used with a good seal use protocol can potentially provide good tamper detection. Sophisticated seals used poorly will not.[2,13,19-22]

**Choosing & Procuring Seals**

In choosing a seal, it is important to realize that there is no such thing as an unspoofable seal (any more than there is an undefeatable lock). There is also no one "best" seal. The optimal choice of a seal depends on details of your security goals, threats, adversaries, personnel and their training, as well as the nature of your containers, doors, hasps, physical facilities, and time and budget constraints.

Generally, seals that are complex, difficult to use, or that present significant ergonomic problems will be resisted by seal installers and inspectors and will not provide good security.

All seals need a unique identifier, such as a serial number, so that an adversary cannot easily swap one seal for another. Independent parts of seal should have (ideally the same) serial number. Serial numbers should not be easy to erase, dissolve, or buff out (though they often are).

Seal vendors and manufacturers (ideally) should contractually agree not to sell duplicate serial numbers or replicate logos to anybody (even within your organization!) who are not on your organization's short list of authorized seal buyers. Seal users should test if this agreement is honored. Often it is not.

If the seal is frangible, be sure to consider environmental conditions and any rough handling the seal may be receive. Also bear in mind that robust seals on moving containers can be a safety hazard in that they can gouge eyes or skin, or entrap clothing.

Seals should not be chosen based solely on unit cost. There are often much higher costs associated with seal installation, inspection, removal, and training. With reusable (typically electronic), seals, be sure to factor in the cost of unit failures, battery replacement, and theft/loss/vandalism of the seal, as well as the costs of protecting and returning the seals for re-use (if necessary).

**Seal Installation**

Unused seals must be carefully protected prior to use, not just left lying around a loading dock, for example. Seals should be assigned to specific individuals who are responsible for protecting and returning unused seals. Unused seals are potentially very useful to an adversary for practicing attacks, or for use in an attack.

Prior to installation, a seal should be checked for manufacturing defects and for evidence of pre-installation tampering (a "backdoor attack") which can make it easier for an adversary to open the seal later without leaving evidence.

The door, hasp, or locking mechanism, as well as all sides (and top and bottom) of the container must be inspected. It makes little sense to seal a container with gaping holes in it, or to apply a seal to a door, hasp, or locking mechanism that is faulty. (You'd be surprised, however, how often people do this!)

Seals should not be used in sequential order. Adversaries must not be able to guess a seal serial number in advance, or even a narrow range of serial numbers!

**Seal Inspection & Removal**

The common misconception that a seal will either be missing or blatantly smashed open, or else there has been no unauthorized access or tampering couldn't be more wrong.[9,14,21] In fact, even amateurs can attack seals in a way that leaves little (and sometimes no) evidence.[9,14,20] Only if the seal inspector has some idea of the most likely attack scenarios and knows what specifically to look for on a given seal can she detect tampering with full reliability. Simply checking to see if the seal is intact and maybe has the right serial number is of limited usefulness, unless you are sure there is no potential adversary with an interest in attacking surreptitiously. (A seal is called a "flag seal" when there is no concern about a surreptitious attack. A flag seals is often used to signal an employee not to unnecessarily reprocess a container. It differs from a "tamper-indicating seal" which is meant to deal with covert tampering or intrusion attempts.)

Seal inspectors should have training on the vulnerabilities and most likely attack scenarios for the seals they are using in the context they are using them. They should have hands-on practice detecting seals attacked both blatantly and subtly. Without this training, they cannot do the best job of detecting tampering.

A seal must be inspected carefully before it is removed, as well as after. Before removing the seal, the seal inspector should also check that the seal displays the right amount of movement or "play" between any 2 mated parts.

Seal inspectors should always compare a seal side-by-side with a protected, unused ("control") seal of the same kind. See figure 2. (This is true even for seals read at a distance with an automated reader.) People are fairly proficient at side-by-side comparisons but not very good at remembering exact details, even for familiar objects.. The seal inspector should

compare the seal color, gloss, surface finish, size, and morphology, and also check the serial number size, font, feel, and character alignment.

Seals should be inspected for evidence of repair or cosmetic coverups of holes or cuts. Smelling the seal—especially as it is being opened—is often remarkably effective in detecting the presence of epoxies, adhesives, paints, inks, solvents, or coatings that have been applied to the seal (even months earlier) by an adversary to hide an attack. Alternately, relatively inexpensive, hand-held electronic sensors can detect many of the same chemicals. If there is time during the inspection, rubbing the seal with a wire brush and/or solvent can be very effective at detecting certain kinds of counterfeit seals or seals that have been repaired.

The door, hasp, or locking mechanism of the container, as well as its sides, top, bottom, and ideally insides must be inspected as well to reliably detect tampering.

After a seal is removed, used seal parts must be protected or thoroughly destroyed so that they cannot be used by an adversary for practicing or executing seal attacks. Ideally, the used seals and seal parts should be saved for some period of time to allow a forensics examination should questions arise.

The best seal inspectors seem to have an uncanny sense that something is suspicious about a seal without necessarily knowing what. Such intuition should never be discounted. Security managers should also make sure that seal inspectors are not hesitant to report their concerns. Sometimes the consternation and delays that a suspicious seal creates for superiors, security personnel, and logistics managers makes front-line employees hesitant to raise their concerns.

Seal inspectors should be occasionally tested with deliberately attacked seals, then heartily rewarded if they detect them. This should include both seals blatantly attacked, and seals attacked with more subtle methods.

## Pressure Sensitive Adhesive Label Seals

After having studied hundreds of such seals, we have concluded that pressure sensitive, adhesive label seals do not generally provide reliable tamper detection. People like using these “sticky labels” because they are inexpensive and appear superficially to be easy to install and inspect. They are, however, typically easy even for amateurs to defeat.

If you insist on using adhesive label seals anyway, here are some suggestions:

1. Match the type of adhesive to the surface. The best adhesive for bare metal is not necessarily best for painted metal, plastic, wood, cardboard, paper, or glass.

2. Feel the surface that the seal will be applied to so that you can detect any substances the adversary has added to reduce adhesion. Pre-cleaning of the surface with a solvent or detergent water is strongly recommended. Residue from previous adhesive label seals must be fully removed.

3. The surface should not be cold, wet, corroded, or peeling.

4. Full adhesion requires more than 48 hours. This often makes it easy for the first 2 days to lift the seal without causing damage or evidence of tampering. Heat can help speed up the adhesion process. (For safety reasons, be careful not to heat any cleaning solvent that has not yet fully evaporated!)

5. Ideally the adhesive, substrate, and ink should be made of the same material, or at least they should dissolve in exactly the same solvent. (Few, if any, adhesive label seals are designed this way.)

6. Consider covering the label seal with a plastic protective sheet or clear protective spray while it is in use.

7. During seal inspection, carefully examine the surface area outside the perimeter of the seal to look for evidence of attack.

8. The best way to detect tampering with an adhesive label seal is to observe (and smell) as the seal is being removed. The seal inspector, however, must understand how the seal is supposed to behave (and smell) ordinarily.

9. A blink comparator used with a kinematic mount (to exactly re-position the camera without any necessary adjustment) is an excellent way to compare before and after images of seals to look for tampering. Contact the authors for more information.

10. Manufacturers and vendors often emphasize the unique features of adhesive label seals that they claim are difficult or impossible to replicate. This is usually quite untrue in our experience, but it doesn't usually matter since most adhesive label seals will be attacked by reusing the original seal, perhaps with some artistic, cosmetic, or repair work.

11. Seals that reveal words like "OPENED" or "VOID" or show patterns when removed from a surface are largely gimmicks that do not represent serious challenges to an adversary. (On the other hand, this feature can be quite effective for flag seals.)

## ISO 17712

In our view, existing standards for tamper-indicating seals are not very helpful. We believe that ISO 17712, the new international standard for freight seals [24], does a particularly serious disservice to effective tamper detection. ISO 17712 formalizes flawed concepts, encourages misleading terminology, over simplifies critical seal and vulnerability issues, and compromises cargo and homeland security. We are preparing a detailed critique of this standard but our advice in the meantime is not to be overly confident about seals that meet the ISO 17712 standard.

## Better Seal Training

The best advice and training for tamper detection is specific to the relevant seals and the security application of interest. The authors are available to provide seal and cargo security advice for legitimate organizations that face security and tampering issues.

## Conclusion

If used effectively (i.e., with a good use protocol) and with a realistic understanding of their capabilities and vulnerabilities, seals can provide fairly reliable tamper detection. But they are not a simple-minded, silver bullet for tamper detection or logistics security. We also believe that much better seal designs are possible.[2,5,11,17]

## Disclaimer

The views expressed here are those of the authors and should not necessarily be ascribed to Argonne National Laboratory or the United States Department of Energy.

## About the Authors

Roger Johnston, Ph.D., CPP and Jon Warner, Ph.D. are part of the Vulnerability Assessment Team (VAT) at Argonne National Laboratory.[15,17] The VAT has provided consulting, training, vulnerability assessments, and security solutions for over 50 government agencies and private companies. Johnston and Warner have conducted vulnerability assessments on hundreds of different seals, and demonstrated easy-to-exploit vulnerabilities (but also effective countermeasures) for many other physical security devices and systems including locks, tags, access control and biometrics devices, GPS, RFIDs, nuclear safeguards, and electronic voting machines.

Dr. Johnston and Dr. Warner have published more than 170 technical papers, given over 90 invited talks (including 6 Keynote Addresses at national and international security conferences), and hold 10 U.S. patents.

## References

1. RG Johnston, DD Martinez, and ARE Garcia, "Were Ancient Seals Secure?", *Antiquity* **75**, 299-305 (2001).

2. RG Johnston, "Tamper-Indicating Seals", *American Scientist* **94,** 515-523 (2005).

3. NAVFAC, "Department of Defense Lock Program: Security Seals", https://portal.navfac.navy.mil/portal/page/portal/navfac/navfac_ww_pp/navfac_nfesc_pp/locks/SEALS_INFO/TAB_SEALS_INTRO.

4. RG Johnston, "The Real Deal on Seals", *Security Management* **41**, 93-100 (1997).

5. RG Johnston, "The 'Anti-Evidence' Approach to Tamper-Detection", *Packaging, Transport, Storage & Security of Radioactive Material* **16,** 135-143 (2005).

6. RG Johnston, "New Research on Tamper-Indicating Seals", *International Utilities Revenue Protection Association News*, **16**(1), 17-18 (2006).

7. L Tyska, Editor (1999), "Seals" in *Guidelines for Cargo Security & Loss Control*, (National Cargo Security Council, Wash, D.C.), Chap 4 (29-38).

8. U.S. Nuclear Regulatory Commission, "Pressure-Sensitive and Tamper-Indicating Device Seals for Material Control and Accounting of Special Nuclear Material", Regulatory Guide 5.80, December 2010, http://pbadupws.nrc.gov/docs/ML1018/ML101800504.pdf

9. AW Appel, "Security Seals on Voting Machines: A Case Study", *ACM Transactions on Information and System Security*, 14(2), September 2011, http://dl.acm.org/citation.cfm?id=2019603&CFID=63720906&CFTOKEN=32687086

10. RG Johnston, EC Michaud, and JS Warner, "The Security of Urine Drug Testing", *Journal of Drug Issues*, **39**(4) 1015-1028 (2009).

11. RG Johnston, "Tamper-Indicating Seals for Nuclear Disarmament and Hazardous Waste Management", *Science and Global Security* **9,** 93-112 (2001).

12. RG Johnston, "Tamper Detection for Safeguards and Treaty Monitoring: Fantasies, Realities, and Potentials", *Nonproliferation Review* **8**, 102-115 (2001).

13. RG Johnston and JS Warner, "The Doctor Who Conundrum: Why Placing Too Much Faith in Technology Leads to Failure", *Security Management* **49**(9), 112-121 (2005).

14. AW Appel, "The Trick to Defeating Tamper-Indicating Seals", https://freedom-to-tinker.com/blog/appel/trick-defeating-tamper-indicating-seals

15. P Rogers, "Most Security Measures Easy to Breach", http://www.youtube.com/watch?v=frBBGJqkz9E

16. JS Warner and RG Johnston, "Why RFID Tags Offer Poor Security", *Proceedings of the 51st Annual INMM Meeting,* Baltimore, MD, July 11-15, 2010.

17. Argonne National Laboratory, "Vulnerability Assessment Team", http://www.ne.anl.gov/capabilities/vat.

18. RG Johnston, ARE Garcia, and AN Pacheco, "Efficacy of Tamper-Indicating Devices", *Journal of Homeland Security*, April 16, 2002, http://www.homelandsecurity.org/journal/Articles/displayarticle.asp?article=50

19. RG Johnston and ARE Garcia, "Vulnerability Assessment of Security Seals", *Journal of Security Administration* **20**, 15-27 (1997).

20. RG Johnston, "Effective Vulnerability Assessment of Tamper-Indicating Seals", *Journal of Testing and Evaluation* **25**, 451-455 (1997).

21. RG Johnston, ARE Garcia, and WK Grace, "Vulnerability Assessment of Passive Tamper-Indicating Seals", *Journal of Nuclear Materials Management* **224**, 24-29 (1995).

22. RG Johnston, "Assessing the Vulnerability of Tamper-Indicting Seals", *Port Technology International* **25**, 155-157 (2005).

23. RG Johnston and ARE Garcia, "An Annotated Taxonomy of Tag and Seal Vulnerabilities", *Journal of Nuclear Materials Management* **229**, 23-30 (2000).

24. International Standards Organization, "Freight Containers – Mechanical Seals", ISO 17712, September 1, 2011.

## Figures

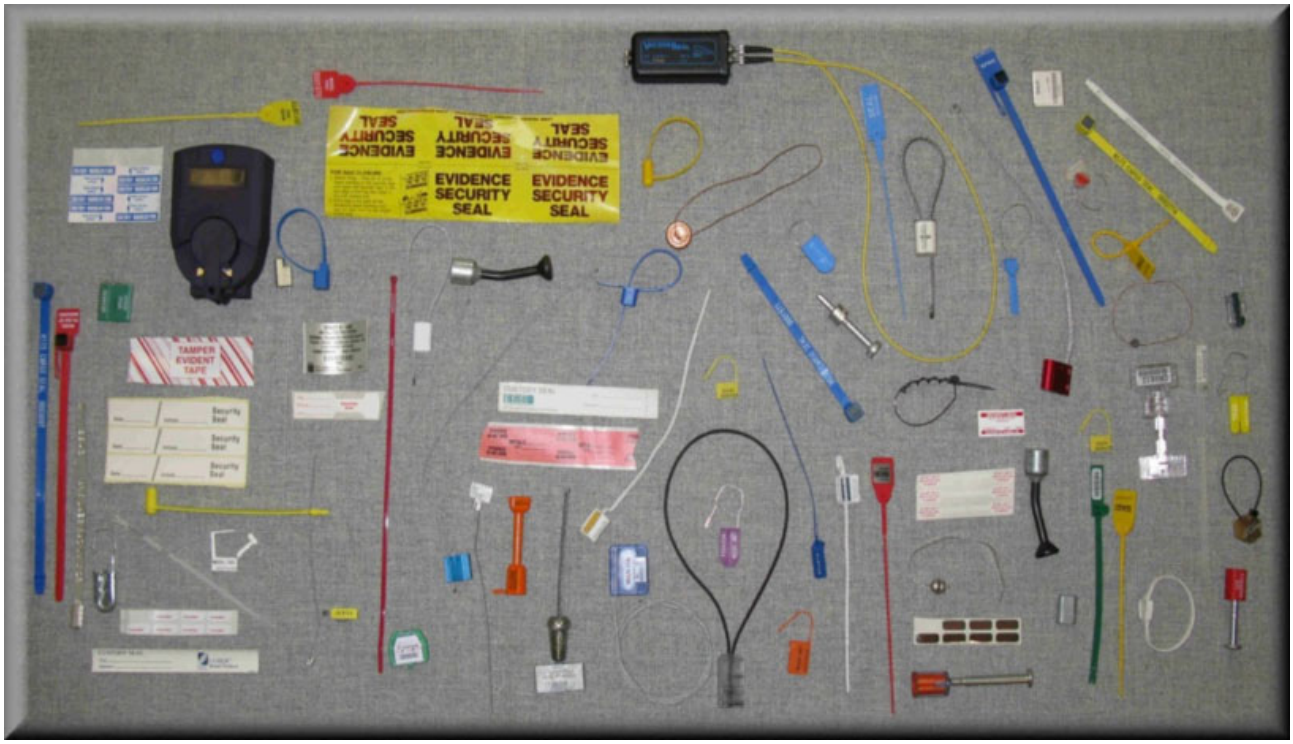



Figure 1 - Examples of the more than 5,000 tamper-indicating seals that are commercially available. Some are based on supposedly irreversible mechanical assemblies. Others are frangible or use electronic or optical means to detect physical intrusion or seal opening. Adhesive label seals typically attach to an object or container using a pressure-sensitive adhesive.

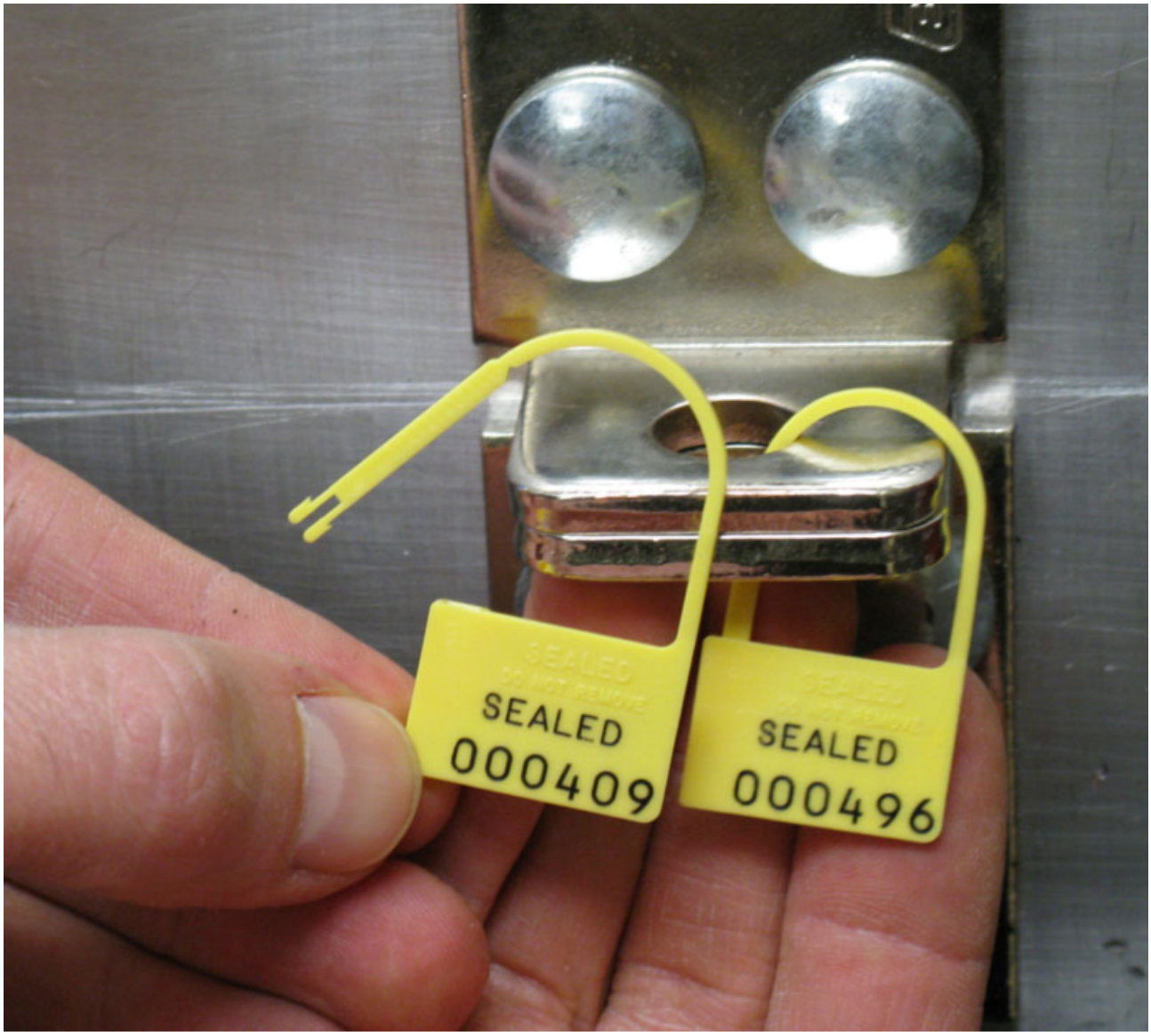



Figure 2 - At inspection time, a seal should be compared side-by-side with a similar, unused seal that has been protected from tampering.

Journal of Physical Security 6(1), 32-42 (2012)

# ELECTION SECURITY: DON'T START WITH FRAUD INVESTIGATIONS, START WITH SECURITY INVESTIGATIONS

SHARON MERONI
Executive Director
Defend the Vote

Telephone: 847-382-1100

Sharon@DefendTheVote.com


## KEYWORDS

ELECTION SECURITY, ELECTION AUDITING, ELECTION INTEGRITY, DEFEND THE VOTE, AUDIT THE VOTE, CHICAGO ELECTIONS, CHICAGO BOARD OF ELECTIONS, SUBURBAN COOK COUNTY ELECTIONS, ILLINOIS STATE BOARD OF ELECTIONS, ARGONNE NATIONAL LABORATORY, VOTING, ELECTION INTEGRITY, ELECTIONS, AUDIT, ILLINOIS, SHARON MERONI

We should be unfaithful to ourselves if we should ever lose sight of the danger to our liberties if anything partial or extraneous should infect the purity of our free, fair, virtuous, and independent elections.

-- John Adams

## INTRODUCTION

This is a follow-up report related to the paper "Vulnerability Assessment and Security Audit of Election Day Polling Place Procedures for the April 5th 2011 Municipal Election in Chicago, Illinois" [Journal of Physical Security 5(1), 12-72 (2011)]. In 2011, this audit and subsequent report looked at polling place procedures in place in Chicago precincts both from the perspective of how well the security procedures were followed and how effective the measures were in securing the vote.

The 2011 study involved visiting 239 precincts on Election Day.[i] The findings were that 210 precincts (91%) failed on one or more of the 11 security measures they were evaluated for; most failed on more than one security item. In 139 instances, election judges and Chicago Board employees failed to seal the ballot box. In a follow up review of the procedures, Roger G. Johnston, Ph.D., CPP, expressed the view that the "Chicago Board of Elections security protocols are wholly inadequate in securing the ballot."[ii]

Following the publication of the 2011 study in the Journal of Physical Security, critical security changes were made in election procedures by the Chicago Board of Election Commissioners (CBEC). The CBEC administers elections in the City of Chicago. The Suburban Cook County Clerk, David Orr (D), administers elections to Suburban Cook County, but not to Chicago.

This paper will review these developments and changes, discuss ongoing challenges in security at Suburban Cook County Elections, present information about ongoing investigations and preparations in advance of the 2012 elections, and briefly discuss broader implications and next steps.

## DEVELOPMENTS AT THE CHICAGO BOARD OF ELECTION COMMISSIONERS

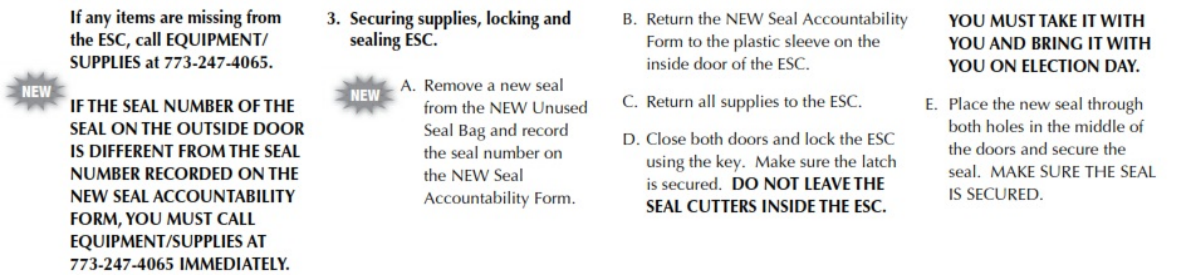
On Wednesday, February 28th, 2012, members from Defend the Vote and other concerned Chicago voters addressed the Chicago Board of Elections Commissioners (CBEC) about security lapses found as a result of the April 5th 2011 audit of 239 precincts in Chicago. At the February CBEC meeting, we were informed that the Board acted on more than one of the critical security changes recommended by Defend the Vote and Dr. Roger Johnston in the Journal of Physical Review. These changes closed some of the holes in security procedures protecting the ballot and the balloting equipment.[iii] These changes impact procedures during Early Voting and on Election Day.

Early Voting: In 2010 investigators discovered that Chicago used non-citizens to operate some early voting sites. This discovery came with the revelation that the CBEC used employees to run early voting sites and that the employment documents for many of these employees were severely deficient. (Federal I-9 Employment Eligibility Forms were not

properly filled out.) In addition, while employees do not have to be US Citizens, election judges do. In the past, employees at early voting sites reported to one person who also wrote their performance reviews. This practice is problematic for a multitude of reasons, not the least of which because it creates a security risk when polling place authority is centralized through one person. The investigation found an instance at an early voting site in Chicago, where the polling place supervisor was a non-citizen and a political activist for open borders.[iv]

Changes implemented at the Chicago Board of Election Commissioners include:

1. All early voting locations in Chicago now have a Republican and Democrat Election Judge overseeing the election.
2. Increased access for party officials to schedule election judges.
3. Chicago Democrat or Republican committeemen now pick the early voting judges.
4. All employees operating the 50 or so early voting sites in Chicago are now registered voters. Registered voters must *a priori* be USA citizens.
5. Implementation of procedures in the Human Resource Department including re-vamping I-9 Employment Verification procedures:
    a. In March 2012, a follow-up FOIA request for the I-9 forms of all employees operating early voting found the new employee verification forms are 99% compliant. This is a complete reversal from 2011 where the forms were found to be 75% non-compliant.
6. New seals with additional bar-code verification procedures assuring that seals are not disturbed.
    a. The ESC (Equipment Supply Carrier) was secured with thin numbered plastic seals, and the numbers were not tracked. The CBEC has implemented a new bar scan code seal tracking system that verifies and tracks the ESC from the warehouse, until the election judges open the equipment, and when returned to the warehouse. The new seal has been upgraded to a strong plastic loop numbered seal that must be clipped open.
    b. These new seals are more difficult to compromise. The serial numbers of the seals are now recorded and verified which closes a major security loophole. In addition, used and unused seals are returned to the election board after the elections. See figures 1 and 2.



If any items are missing from the ESC, call EQUIPMENT/ SUPPLIES at 773-247-4065.

NEW

IF THE SEAL NUMBER OF THE SEAL ON THE OUTSIDE DOOR IS DIFFERENT FROM THE SEAL NUMBER RECORDED ON THE NEW SEAL ACCOUNTABILITY FORM, YOU MUST CALL EQUIPMENT/SUPPLIES AT 773-247-4065 IMMEDIATELY.

3. Securing supplies, locking and sealing ESC.

NEW

A. Remove a new seal from the NEW Unused Seal Bag and record the seal number on the NEW Seal Accountability Form.

B. Return the NEW Seal Accountability Form to the plastic sleeve on the inside door of the ESC.

C. Return all supplies to the ESC.

D. Close both doors and lock the ESC using the key. Make sure the latch is secured. **DO NOT LEAVE THE SEAL CUTTERS INSIDE THE ESC.**

**YOU MUST TAKE IT WITH YOU AND BRING IT WITH YOU ON ELECTION DAY.**

E. Place the new seal through both holes in the middle of the doors and secure the seal. MAKE SURE THE SEAL IS SECURED.

Figure 1: New instructions from the Chicago Board of Elections Judge Training Guide: March 2012

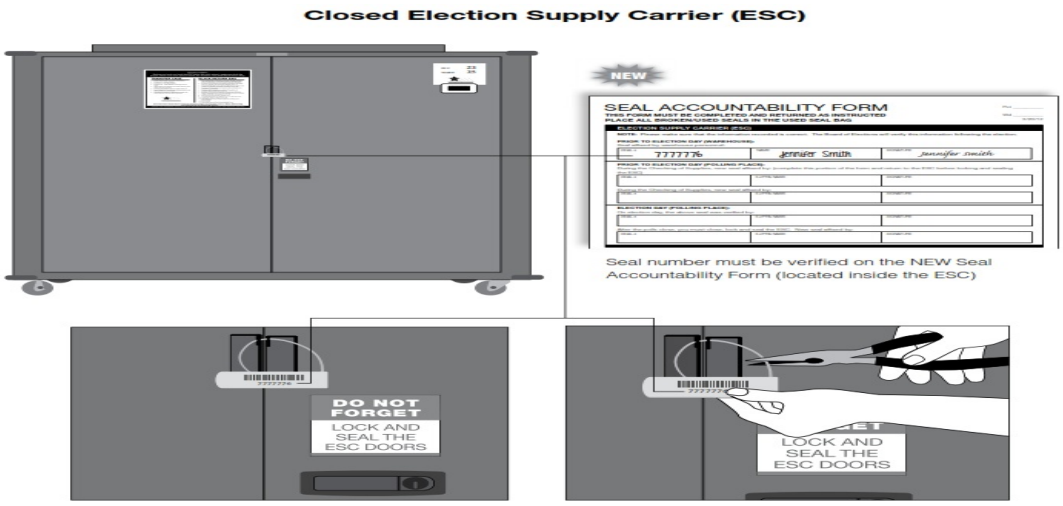



Figure 2: The Equipment Supply Carrier (ESC) and the new Seal Accountability Form. The new plastic seals have a bar-coded number and must be clipped open.

7. Updated seal procedures:
    a. A new bag for "unused seals" is located on the door of the ESC. After the polls close, this bag is returned in the sealed ESC.
    b. A new bag for "used seals" is located on the door of the ESC. All used seals must be included. After the polls close, this bag, along with the seal accountability form, is returned in the sealed black bag that contains other critical items such as memory devices.
    c. Three new seal accountability forms were added. These forms are started at the warehouse when the equipment is sealed; custody of these forms is maintained through the sealed ESC. The judges or the PPA (Polling Place Administrators, who are Board employees) verify seals before the election open. After the election, the forms are returned and sealed inside the black bag.
    d. New seal procedures include verification of the numbers on seals protecting the election equipment. This is now complaint with Illinois statutes. See figure 3.
    e. Seal procedures require notification of the election officials if they are compromised.

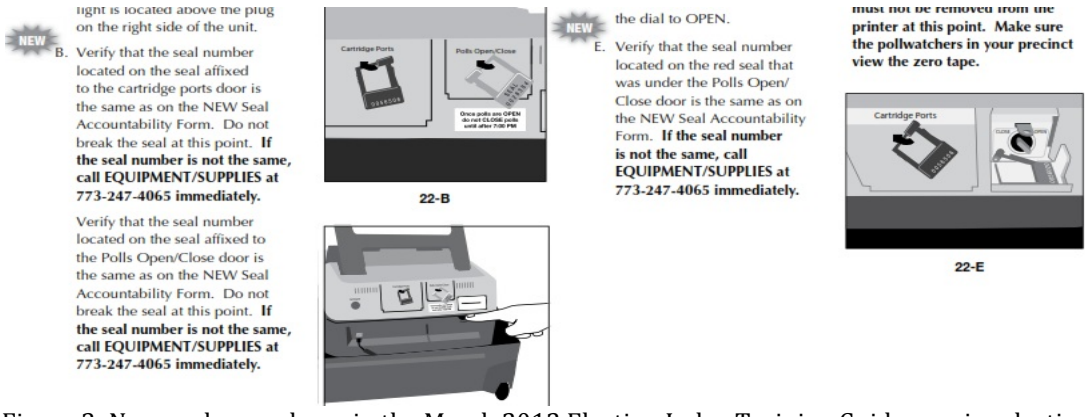



Figure 3: New seal procedures in the March 2012 Election Judge Training Guide require election judges verify seal numbers and report if it is not the correct number.

f. Instructions for sealing the ballot box now include pictures. The audit investigation learned that most election judges were not aware they had to seal the ballot box. Enhanced instructions close that gap in training, especially when combined with the new processes of seal recording, verification, and returning used and unused seals to election authorities. See figure 4.


Figure 4: Instructions illustrating how seals are attached, requiring seal numbers are recorded.

## SECURITY CHALLENGES - SUBURBAN COOK COUNTY BOARD OF ELECTIONS

There are very specific Illinois laws in place specifying how election equipment is to be managed. These laws serve to provide a measure of system-wide security throughout the Illinois voting system. In March 2012, while comparing some of these laws with Suburban Cook County Elections' procedures, Defend the Vote investigators uncovered that Suburban Cook County procedures were not complaint with Illinois statues. The Defend the Vote investigation concluded that elections in Suburban Cook County Elections are being conducted unlawfully because they technically fail to comply with Illinois statute. The legal remedy these statues provide for is the following: either the poll shall not open or the ballot shall not be counted until the deficiency is corrected.

These deficiencies are system-wide and require a change in procedures for Suburban Cook County Elections to be lawful[v].

In brief, a few of the legal issues:

i. **Voter Supply Carriers:** Suburban Cook County Elections' Voter Supply Carrier (VSC) is similar to Chicago's ESC. They contain election material before, during, and after voting. When stored at in-precinct voting centers, the VSC's are not required to be stored in a locked room. The VSC's are delivered to these locations approximately a week before the elections. There isn't a paper or seal tracking system securing the chain of custody of the equipment during this time period.

   Illinois law attempts to secure the ballot inside all election supply carriers by strictly securing the key locking these containers, and by sealing the VSC along with sealing each voting device within it.

In Suburban Cook County, the VSC has a universal key securing the election materials and the equipment stored inside. This key is sent home in unsealed envelopes with Equipment Manager Judges for lengths of time of up to 10 weeks. The VSCs are locked with this universal key, but are not sealed.

Illinois statutory procedures for these keys include that all election judges sign off after observing the unsealing of the package containing the key. This procedure is not followed. Illinois law requires a verified chain of custody and specifies the polls shall not open if the procedures as set out in the statute are not followed. (10 ILCS 5/24-13 from Ch. 46, par. 24-13)[vi]

ii. **Unsealed Memory Devices:** The memory device in the ballot scanner is unsealed. On the eve of elections, the training instructions tell Cook County election judges to leave this unsealed ballot scanner out overnight as part of the polling place set-up procedures. The scanner is partially contained in the locked VSC. The locked VSC is not sealed and has a universal key.

Following the election, the same memory devices-now containing the record of the scanned paper ballots-are returned to election authorities in unsealed bags.

iii. **Sealing of the Ballot Box:** Suburban Cook County Elections set-up procedures instruct that ballot boxes are to be set-up, sealed, and left out overnight. The seals on these ballot boxes are recorded the night before the election, but are not verified at any point during the election process.

These ballot boxes are not opened and declared empty in the public space in front of pollwatchers, as Illinois law requires.[vii]

iv. **Sealing of the Voted Paper Ballot:** According to Suburban Cook County Election procedures, paper ballots are initially counted in unsealed wrapped packages the night before the elections. These unsealed wrapped ballots are stored in the unsealed VSCs before the election.

Voted paper ballots are transported after the election, unsealed and unwrapped, in an unlocked but sealed carrying case.

"Ballots returned to the office of the election authority are not signed and sealed as required by law **shall not** be accepted by the election authority until the judges returning the ballots make and sign the necessary corrections." (emphasis added) 10 ILCS 5/24A-10.1 from Ch. 46, par. 24A-10.1

After the election, Illinois law requires voted paper ballots to be wrapped with tape in a cross like pattern and sealed with all of the judges' signatures affixed before being placed in a sealed and locked carrying case so the ballots can be moved without being disturbed. This mandated security procedure is ignored in Suburban Cook County.[viii] See figure 5.

Figure 5: Ballots should be returned to the election authorities in a sealed bag, such as this one containing voted ballots at the Chicago Board of Election Commissioners Pershing Ave Warehouse.

The blue case is locked and sealed by election judges before leaving the polling place.

v. **Voter Privacy:** The Voter Verified Paper Audit Trail (VVPAT) on the electronic voting machines acts as another layer of security. Presumably, this paper trail ensures the voter's choice is correctly recorded and allows for voters to verify and observe the printing of this paper ballot as their vote is recorded. The machine records this vote electronically and on the paper scroll inside the printer. The voter does not get a copy.

   Investigations have uncovered that Suburban Cook County Elections generates PDF copies of this VPPAT scroll, which is electronically searched while auditing votes during candidate challenges. This raises another security issue, which is the privacy of the vote.

   Electronically, everything is coded and traceable with search parameters. Access to this data is controlled, but is it secure? If voter choices can be traced to their electronic ballot based on the digital code that is associated with their ballot, then what security measures are in place to protect voter privacy from the operators of the system or from electronic hackers?

   The broader question is have we moved into electronic voting with sufficient controls to ensure the privacy and integrity of the vote? Our ongoing investigations examine this.

## ONGOING INVESTIGATIONS AND PREPARATIONS FOR THE 2012 ELECTIONS

**1) Polling Place Security Assessment Forms**: Following the April 2011 audit, Defend the Vote initiated a program to audit the security of elections across the state of Illinois. To accomplish this, assessment criteria must accommodate individual election jurisdictions' procedures.

The administration of elections is conducted at the election jurisdictional level. However, the Illinois State Board of Elections (ISBE) has clear oversight and approval over all instruction manuals which are used to instruct Illinois election judges. Consequently, there will be similar state-wide procedures overall, with local variations that must be approved by the ISBE.

The framework to accomplish this security assessment has been set up. A base form has been designed which is then adapted for specific election jurisdictions. These forms are designed based on Illinois State Board of Elections' instruction manuals and the type of equipment

used[ix], and based on individual election jurisdictions' procedures. One of the challenges in this project is to design forms in synergy with election jurisdictions. Many times, they are in the process of re-designing procedures right before an election; there are always last minute changes!

The distribution of Polling Place Security Assessment Forms is another one of our challenges. Our objective is to distribute forms to as many polling places across Illinois as possible. We also want to inform while we are assessing because this encourages a security culture in the polling place.

One of our strategies to do this is to develop non-partisan security-based training videos for election judges and poll watchers, and to make these videos available publically. We will reach out though the various political parties and encourage them to use these videos and related information as part of their GOTV and election judge campaigns. We will also distribute these videos to the election jurisdictions and to community groups. They will be viewed online and through DVDs. The Chicago Board of Election Commissioners has agreed to link to these training videos from their website. We will encourage other election jurisdictions to do the same.

Along with these training videos, we will distribute the Polling Place Security Assessment Forms. Our distribution strategy includes sending them out to election authorities, both political parties, and a variety of community groups, and by making them available online. These security assessment forms are designed to be filled out by pollwatchers and election judges because they have greater access to view election equipment than the average voter.

**2) Voter Assessment Forms:** We are developing Voter Assessment Forms that specifically asks voters to provide feedback on their voting experience. The objective of these forms is to encourage voters to be aware of security in their polling place and to set up a process by which voters can assess and report back about their voting experience. Defend the Vote piloted this form in the 2012 Primary, and has adapted the form for the November election. The Voter Assessment Form will be published online and sent out through various community and political groups beginning in September. These forms are non-partisan and will be available regardless of political affiliation.

In addition to the Voter Assessment Form, we will produce "Voter Awareness" videos that provide insight into what to look for in the polling place. These videos will be available free online, and on CDs.

**3) Vulnerability Assessment of Cook County, Chicago and Across Illinois:** Beginning at the end of August and going through September, Defend the Vote has arranged for Argonne National Laboratory's Vulnerability Assessment Team to work with Chicago and Cook County to review their election systems strictly from a security perspective. Also participating, the Illinois State Board of Elections has provided information on the certification of election equipment used throughout Illinois. They will continue to provide information as needed during this assessment period. Ultimately, Defend the Vote wants to assess all election systems and procedures in Illinois strictly from a vulnerability and security perspective. It will take more than one election cycle to conduct this assessment state-wide.

The overall strategy of this vulnerability assessment is to work with local election officials and state legislators to increase election security in Illinois. The impact is to increase the security and the security culture in elections, and to increase voter confidence in the integrity of elections.

## BROADER IMPLICATIONS

Elections are a local matter with national consequences. Securing elections is not a simple matter, and it requires establishing a culture within the State: an election security culture. Across Illinois, voters entrust election security to the political parties and to their elected County Clerks or Election Commissioners. Our investigations show that election law is not uniformly practiced or enforced in Illinois. Citizens have an essential role in election security.

Establishing a security culture in Illinois elections cannot be accomplished in one election, nor can we ever consider election security to be a done deal. It is an evolving process. This process is complicated by the increasingly complex (and changing) ways the vote is cast. Access to information is key to developing an open election security culture.

Besides looking at the processes for Election Day voting, there are numerous ways to cast the ballot that are designed to encourage voter access to voting. In Illinois, voters can cast a ballot by voting early, absentee voting, grace period voting, and provisional voting. These different methods of voting have different security risks associated with safe guarding the vote. These risks include chain of custody of the ballots and the security of the software and machines tallying these votes.

As Defend the Vote investigates election security in Illinois, we will be looking at the entire process which includes ballots, machines, software, warehousing, transportation, and repair of election equipment and materials. We will work with this information to encourage a security culture as we design next steps.

## NEXT STEPS

Next steps include working with election jurisdictions on security. We are researching physical and electronic security, and processes and procedures involved in securing the vote. We are encouraged that many election authorities are willing to have their procedures reviewed. It has been our experience that County Clerks in Illinois do care about the integrity of the vote they safeguard.

We are also launching election judge, pollwatcher and voter education programs. We believe an informed electorate is the first line of defense in ballot security. Open access to information is key to developing a security culture in elections.

A fresh look at the integrity of the vote through studying, refining, and enforcing security procedures in place will make a difference in not only securing the vote, but also in assuring the public that the integrity of the vote means their vote DOES matter. Nothing destroys voter enthusiasm and consequently voter participation in elections more than a belief that their vote doesn't count.

Overall, the success of these citizen-based election integrity investigations in Illinois is a great story. These successes reinforce that election security is always a local matter requiring voter participation as part of the equation that keeps their vote secure.

Our advice is simple: Don't start with fraud investigations, start with a security investigation!

## ACKNOWLEDGEMENTS

Funding Bodies: Champion News and Jack Roeser, Chairman of Otto Engineering.

"I am an active supporter of Defend the Vote and encourage voters and groups across the state to expand our investigations by joining in the first citizen-run audit of Illinois elections." Jack Roeser**,** Publisher of Champion News, President of the Family Taxpayers Foundation and Chairman of Otto Engineering

Roger G. Johnston, Ph.D., CPP, head of the Vulnerability Assessment Team (VAT) at Argonne National Laboratory, was invaluable for his advice and expertise on election security.

Thank you to the anonymous peer reviewers for the Journal of Physical Security who helped to make this report stronger and who approved it for publication.

## REFERENCES

Suburban Cook County Elections, *The Equipment Manager Handbook for the March 20, 2012 Primary Election*

Cook County, *Equipment Manager Video*, http://www.cookcountyclerk.com/newsroom/newsfromclerk/Pages/EquipmentManagerResources.aspx

Chicago Board of Elections Commissioners, *The Judge of Election Handbook for the March 2012 Elections*

Suburban Cook County Elections, *The Judge of Election Handbook for the March 2012 Elections*

## NOTES

[i] The Journal of Physical Security 5(1), 12-72 (2011), http://jps.anl.gov/

[ii] Meroni, Sharon. Chicago Board of Elections is "Wholly Inadequate" in Protecting the Vote! October 5, 2011 www.DefendtheVote.com This web article discusses the first audit.

[iii] Meroni, Sharon. Kudos to the Chicago Board of Election Commissioners March 9, 2012. www.defendtheVote.com . This article goes into greater depth on the changes made by the Chicago Board of Election Commissioners.

[iv] Eloise Gersten. Chicago GOP Letter to the Chicago Board of Elections. June 13, 2011. www.DefendtheVote.com. and Meroni, Sharon. Early Voting Polling Places in Chicago are Being Run by Non-Citizens. June 13, 2011. Both articles reference in greater detail the problems uncovered at early voting locations in Chicago in 2011.

[v] Meroni, Sharon. David Orr Disregards Illinois Law. February 29th, 2012. www.DefendtheVote.com .

[vi] There are two passages to involved in 10 ILCS 5/24-13 from Ch. 46, par. 24-13

"No precinct election official shall break the seal of such envelope except in the presence of all members of the precinct election board, and such envelope shall not be opened until it shall have been examined by each member of the precinct election board to see that it has not been previously opened. Such envelope shall not be opened until it shall have been found that the numbers and records recorded thereon are correct and agree in every respect with the numbers and records as shown on the machine. "

And

"... that the machine is otherwise in perfect order and they shall compare and record the number on the metal seal with which the voting machine is sealed, with the number furnished them as recorded on the envelope containing the keys, by the election authority, and if the number on the seal and the number on the protective counter do not agree with the numbers supplied to them, they shall not open the polls"

[vii] There are at least two statutes involved. 10 ILCS 5/17-3 from Ch. 46, par. 17-3 and 10 ILCS 5/24-8 Ch. 46, par. 24-8.

(a) Before voting begins, the ballot box shall be publicly opened and exhibited, and the judges shall see that no ballot is in such box; after which the box shall be locked and the key delivered to one of the judges, and shall not be again opened until the close of the polls. This paragraph (a) applies whenever permanent type ballot boxes are used, and does not apply when non-permanent type ballot boxes are used in accordance with section 15-1, paragraph (b).

(b) When non-permanent type ballot boxes are used in accordance with section 15-1, paragraph (b), prior to the commencement of voting and before any ballots are deposited therein, the judges shall examine each sealed ballot box, show it to those present and insure that it is in fact sealed and empty; the sealed slot shall be broken open before those present and the box inspected to insure that it is empty and such ballot box shall not be removed from public view from the time it is so inspected until after the close of the polls. The sealed opening on the side of the box shall not be unsealed or opened until after the close of the polls. 10 ILCS 5/17-3 from Ch. 46, par. 17-3

Pollwatchers as provided by law shall be permitted to carefully check the voting machine and its protective devices, and ballot labels and registering counters, before the polls may be declared open on election morning, and they shall be permitted to remain in the polling place at all times throughout the conduct of the election if desired, and after the close of the polls, to be present and check the protective devices and registering counters of each voting machine, and the official return sheets thereof. 10 ILCS 5/24-8 Ch. 46, par. 24-8

[viii] ...however, that such container must first be sealed by the election judges with filament tape provided for such purpose which shall be wrapped around the container lengthwise and crosswise, at least twice each way, in such manner that the ballots cannot be removed from such container without breaking the seal and filament tape and disturbing any signatures affixed by the election judges to the container. (10 ILCS Sec.24A-10.1) and (10 ILCS 5/24B-10.1) and (10 ILCS 5/24B-15.01)

[ix] Illinois uses 7 election systems which are certified and currently in use in various combinations across Illinois: The M100, AutoMARK, Accuvote, TSX, Edge2Plus, InsightPlus, and eSlate. Election systems in use can be viewed at http://www.elections.il.gov/votinginformation/votingeq

Viewpoint Paper

# Common Election Security Myths*

Roger G. Johnston, Ph.D., CPP
Vulnerability Assessment Team
Argonne National Laboratory

After talking with dozens of different election officials around the country, I've come to the conclusion that the following myths about election security are quite common.

**Myth 1. Tamper-indicating seals will be blatantly damaged or missing if there has been an attack.**

The reality: Stealing votes generally requires surreptitious attacks; tearing off seals is mere vandalism, not a credible attempt at vote stealing. Moreover, even amateurs can attack seals and leave little or no evidence.

Though they rarely get it, seal inspectors (and installers) need at least a few minutes of hands-on training, specific to the relevant seal(s) and application. (See paper #3 about seals in this issue of the *Journal of Physical Security*.)

**Myth 2. Electronic voting machine security is the main issue.**

The reality: The main issue, I believe, is having a healthy Security Culture. The fact that current electronic voting machines have little to no security built in is really part of a weak security culture, where manufacturers are not held accountable by their customers for making secure machines. Some of the other critical attributes of a healthy Security Culture include a strong focus on security, a willingness to think like the bad guys, openness to criticism and suggestions, and avoidance of denial.

**Myth 3. "Certification" and "standards" are of great value for electronic voting machines.**

The reality: Neither are likely to address major election security issues and attack scenarios. Certification and standards are often of minimal use in other security applications, and sometimes make things worse, e.g., ISO 17712 for cargo seals.

*Editor's Note: This viewpoint paper was not peer reviewed.

**Myth 4. Checking that a voting machine seems to be operating properly is an effective security check**.

The reality: In fact, you need to disassemble and reverse engineer the machine to look for signs of tampering and alien electronics. As we in the Vulnerability Assessment Team at Argonne National Laboratory have shown, turning cheating on and off (even remotely) is easy to do.

**Myth 5. Cyber is the only important kind of attack.**

The reality: Actually, other electronic and physical attacks are often easier, harder to detect, and harder to prevent, especially when executed by insiders.

**Myth 6. An adversary has to be very sophisticated to steal votes.**

The reality: Currently, this is clearly not the case in most election jurisdictions.

**Myth 7. Manufacturers of voting machines do a good job with security, and know what they are doing when it comes to security.**

The reality: All one has to do is look briefly at the designs of various electronic voting machines to see that this myth is not true.

**Myth 8. There is little you can do about the insider threat.**

The reality: The insider threat is always a challenge, but there are effective countermeasures that can be implemented.

**Myth 9. Adversaries must tamper with hundreds or thousands of voting machines to succeed.**

The reality: Due to improvements in gauging public sentiment, it is now possible to tell in advance when elections will be very close. In the 2008 Senate race in Minnesota, for example, pollsters predicted an extremely close contest. Indeed, Al Franken won by only 312 votes out of the 2.9 million cast. Tampering with 1-3 voting machines could have changed the outcome of that race. In contests in rural areas or small towns, tampering with a single voting machine might be sufficient.

It is also a fallacy to think that vote tamperers will be only interested in winning an election. Fringe candidates and parties may merely wish to gain credibility, attention, matching funds, or an invitation to future debates by securing, say, 5% of the vote. (The idea stated by some that this is ok as long as it does not affect who wins the election is, in my view, without merit. Even this kind of tampering is still undemocratic fraud that disenfranchises the voters.)

**Myth 10. A Voter Verified Paper Record guarantees there will be no vote tampering.**

The reality: While having a voter verified paper record is an excellent security measure, it does not guarantee election integrity. It just creates an extra step for an adversary. Given the poor protection typically provided for most paper records (including poor seal usage), tampering with paper records is not usually going to be very challenging, especially for an insider.

**"Myth" 11. There has never been a successful cyber, electronic, or physical attack on voting in the United States in recent years.**

The reality: We just don't know. Currently, a competent attack would be unlikely to be detected, especially for the 25% of voters who vote on electronic voting machines that lack a voter verified paper record.

**Myth 12. If I as an election official can't conceive of how to defeat my election security, than nobody can.**

The reality: Few election officials have much experience or expertise with security, and few seem to be highly imaginative. Few get good outside advice about security. (Often, security vendors are their only source of security information.) Few want there to be vulnerabilities—making it hard for them to see vulnerabilities.

Journal of Physical Security 6(1), 46-58 (2012)

# Comparison of Window Stresses from Explosions and Projectiles

David B. Chang (dbcsfc@aol.com)
Consultant
Tustin, California

Carl S.Young (cyoung@strozfriedberg.com)
Managing Director and Chief Security Officer
Stroz Friedberg
32 Avenue of the Americas
4th Floor
New York, NY 10013

## Abstract

Blast film is traditionally applied to windows to reduce the risk of flying glass when subjected to explosion-induced stresses. However, little attention has been paid to the effect of projectiles on windows and understanding potential benefits derived from applying blast film. To that end, simple scaling laws are derived for maximum stresses in windows impacted by both explosive blasts and projectiles such as bullets or rocks. The effect of films and laminations are described, and recommendations are made for safe window designs to protect against both explosive blasts and projectiles. Comparisons are made with typical design recommendations as well as window and film properties.

## 1. Introduction

There is considerable interest in minimizing the effect of explosive-induced forces on glass structures such as windows. Glass fragmentation is one of the significant causes of injury and death in explosive scenarios, and many buildings incorporate some form of window treatment such as lamination, tempering, or application of security films, in order to mitigate this risk.

In addition, projectiles such as rocks and bullets that cause spatially localized and thereby highly concentrated forces upon impact, also pose risk to individuals inside facilities. It is useful, therefore, to understand the effect of standard window treatments on such threats, since these treatments are mostly used to reduce the effect of overpressures and impulses associated with explosive forces.

The purpose of this paper is to summarize a simple theoretical treatment of the problem of window breakage thresholds for both explosive and projectile scenarios. Uncomplicated scaling laws are presented for these thresholds.

Section 2 summarizes the basic analytic approach: the use of a dynamic equation for the distortion of a plate in response to an applied stress, and its solution by a variational principle.

Section 3 describes the maximum stresses developed in an uncoated window of uniform thickness both for an explosive blast and for a projectile.

Section 4 gives the modifications in the results when the window has one or more films or laminations.

Section 5 summarizes the results and compares them with typical design guidelines, window properties, and film properties.

The results are discussed briefly in Section 6.

For ease of reference, the typical design guidelines and window and film properties are summarized in the Appendix.

## 2. Summary of analytic approach

It is not surprising that a window responds differently to an explosive blast than to the impact of a projectile. The blast creates a force over the entire surface of the window whereas the force exerted by a projectile is localized to a small area.

To estimate the breakage thresholds from a blast or projectile, we use an equation that describes the response of a thin solid (a plate) to applied forces.

For a single uniform pane of glass, the dynamic plate equation is

$$(\nabla_x^2 + \nabla_y^2)(\nabla_x^2 + \nabla_y^2) w - (\rho h/D)\partial^2 w/\partial t^2 = P/D \qquad [1]$$

where

w is the displacement perpendicular to the (x,y) plane of the plate
h is the thickness of the plate
ρ is the mass density of the plate
P(x,y, t) is the pressure exerted on the plate

and

$$D = Yh^3/[12(1-\upsilon^2)] \qquad [2]$$

Here,

Y is Young's modulus of the plate
υ is the Poisson ratio of the plate.

Equation [1] is obtained from the familiar static plate equation as given, e.g., in Timoshenko (1940), by adding the term $(\rho h/D)\partial^2 w/\partial t^2$ to account for the inertial effects associated with acceleration.

Although eqs. [1] and [2] only apply to a uniform (i.e., non-laminated) situation, we shall see in Section 4 below that it is straightforward to modify the parameters so as to make eq. [1] applicable to a laminated case as well.

The plate equation is fourth order in the spatial derivatives (in the plane of the plate) and second order in the time derivative. Because it is a linear equation in w, it is useful to Fourier analyze it both in time and space. This is tantamount to describing the motion as a weighted sum over the normal modes of the plate, where the weighting is determined by the time and spatial dependence of the applied pressure P(x,y,t).

For example, when the applied pressure is due to an explosive blast that exerts a uniform pressure over the entire surface of the window, the normal mode that corresponds to the most uniform displacement of the window dominates, with the weighting for the higher normal modes that describe greater spatial variation being much less. When the applied pressure is due to a projectile, again the normal mode that corresponds to the most uniform displacement dominates, since the window experiences a net overall displacement. However, although the weighting for the other normal modes again drops off rapidly, the drop-off is not quite as rapid as for the blast case.

For a window of arbitrary shape, it is useful to employ an integral variational principle form of the plate equation rather than the differential expression of eq. [1] directly. This is because the variational principle form is less sensitive to the exact form of the solution, so that approximate expressions can be used for the displacement w without compromising the results.

To obtain the variational principle, the displacement w(x,y,t) is first Fourier analyzed in the time variable. This introduces the normal mode angular frequency ω. There should exist a Lagrangian for which eq. [1] is the Euler-Lagrange equation. Since eq. [1] is fourth order in the spatial derivatives, it would be expected that the Lagrangian contains second order derivatives.

It is easy to verify that

$$\delta[\omega^2\rho h/D] = 0 \qquad [3]$$

where

$$\omega^2\rho h/D = \iint dxdy\, [\iint(\partial^2 w/\partial x^2 + \partial^2 w/\partial y^2)^2] \,/\, \iint dxdy w^2 \qquad [4]$$

gives eq. [1] as its Euler-Lagrange equation. [See, for example, Courant & Hilbert (1953).]

Equations [3] and [4] are the equations that are used to obtain the results in the following sections, using trial functions for w that are products of the exact normal modes for a 1-dimensional window (where a 1-dimensional window is (a fictitious) one in which w depends only on a single spatial variable).

## 3. Stresses in a uniform clamped rectangular window with no film

The maximum stresses developed in a window with no security film are different for an explosive blast than for a projectile. This is related directly to the more spatially uniform response of the window to a blast than to a projectile.

For a blast, the components of the maximum stress, which occurs at the center of the window, are found to be:

$$\sigma_x(x=y=0) \approx \{Y^{1/2}PT(L_y/L_x)(1-\nu^2)^{1/2}/(h\rho^{1/2})\}[4^5/(3^{7/2}\pi^4)] \qquad \textbf{Blast} \qquad [5]$$

$$\sigma_y(x=y=0) \approx \{Y^{1/2}PT(L_x/L_y)(1-\nu^2)^{1/2}/(h\rho^{1/2})\}[4^5/(3^{7/2}\pi^4)] \qquad \textbf{Blast} \qquad [6]$$

Here the subscripts on the stress refer to the component (direction) of the stress, PT is the impulse per unit area exerted on the window by the blast, $L_x$ is the overall dimension of the window in the x-direction, $L_y$ is the overall dimension of the window in the y-direction, and the other symbols are as defined earlier.

Note that

a. The stresses are independent of the size of the window, depending only on the ratio of the dimensions in the x and y directions. (The independence is because the stress is proportional

to the second derivative of the displacement; and the displacement itself is proportional to the square of the window dimension whereas $\partial^2/\partial x^2$ and $\partial^2/\partial y^2$ are each inversely proportional to the square of the window dimension.)

b. The stresses depend inversely on the thickness of the window, so that thicker windows will have less stress.

c. Interestingly, the stresses are proportional to $(Y/\rho)^{1/2}$, the square root of the Young's modulus divided by the density.

d. The stresses are also proportional to the specific impulse, PT.

The stresses would also be expected to be large at the window edges, especially at the midpoints of the edges. Evaluation of the expressions at those positions show the stresses are comparable to that at x=y=0.

For a projectile impacting the window at its center – i.e. at its most vulnerable point, the maximum stress is found to be:

$$\sigma_x\,(\max) \approx \{Y^{1/2}MV(1-\nu^2)^{1/2}/(h\rho^{1/2})\}[8x3^{1/2}/3\,\pi^2)] \qquad \textbf{Projectile} \qquad [7]$$

$$\sigma_y\,(\max) \approx \{Y^{1/2}MV(1-\nu^2)^{1/2}/(h\rho^{1/2})\}[8x3^{1/2}/3\,\pi^2)] \qquad \textbf{Projectile} \qquad [8]$$

Here, $M_1$ is the projectile mass per unit area of impact and V is the projectile speed.

As with the blast case,

a. The stress is proportional to $(Y/\rho)^{1/2}$, the square root of the Young's modulus divided by the density.

b. The stress is inversely proportional to the window thickness.

It is also interesting to note that:

c. The dimensions of the window do not enter. This might be expected from the localized impact of the projectile.

d. The stress is proportional to the initial momentum $M_1V$. Note, however, that $M_1$ is the mass of the projectile *per unit area of the impact*. This shows that a pointed bullet, or a pointed spear can be more effective in causing damage than a blunt projectile of the same mass.

The magnitude of the numerical factor in the square bracket for the blast case is **0.225**, and the magnitude of the numerical factor in the projectile case is **0.47**.

Thus, we note a two-fold increase in the stress for a given impulse per-unit-area for the projectile compared to the blast case. This is due to the difference in the amplitudes of the normal modes excited in the two cases.

## 4. Stresses in a window with coatings or laminations

The results of the previous section can be modified straightforwardly to describe the effect of laminations or films applied to windows. When a plate is bent, the internal stresses set up inner moments which, with the moments from the inertial forces, counter the external moments on the plate due to the applied pressures. For a plate without laminations, the internal stress at any position (x,y,z) in the plate is directly proportional to the bending curvature, with the proportionality constant depending on the Young's modulus Y, Poisson ratio $\upsilon$, and the bending moment arm (z-h/2).

When laminations are present, the moment arm is changed, and Y and $\upsilon$ also depend on z. Similarly, the density $\rho$ also depends on z, so that the moment of the inertial force needs to take that into account. The net result is that for a laminated window (or a window with one or more layers of film), the earlier equations are modified by simply making the replacements

$$\rho \rightarrow \Sigma_i (h_i / h) \rho_i \qquad [9]$$

$$D \rightarrow \Sigma_i h_i [Y_i / (1-\upsilon_i^2)](z_i - z_N)^2 \qquad [10]$$

where

$$z_N = \Sigma_i h_i z_i [Y_i/(1-\upsilon_i^2)] / \{ \Sigma_i h_i [Y_i/(1-\upsilon_i^2)]\} \qquad [11]$$

Here the subscript i refers to the $i^{th}$ layer in the window, and the summation is over all of the layers (laminations, films)

Our primary focus in this paper is on the ability of a film to hold a shattered window together. In that case, the theoretical treatment is simplified considerably.

Specifically, once the glass is fragmented, to the first approximation we can assume that it will not contribute to the internal bending moments: After it fragments, it only contributes to the mass per unit area. The internal bending moments are then all due to the tension forces in the film.

Accordingly, in the expressions of Section 3, let all the quantities refer to the film alone, except for the density. The density will now be changed to

$$\rho_{effective} \approx \rho_{glass} (h_{glass}/h_{film}) \qquad [12]$$

To reiterate, the rationale for this substitution is that the film now supports all of the inertia and applied forces in the system, with the glass no longer contributing to the internal bending moments. The calculated stress can then be compared to the tensile strength of the film.

## 5. Comparison with typical windows and films

Approximate scaling laws have been derived for the maximum stresses that can be expected in windows subjected to explosions and to projectiles. These have resulted from a variational principle based on a dynamic plate equation. The effect of lamination and films has been included by modifying the parameters appearing in the plate equation.

In this section, the scaling laws of Sections 3 and 4 are compared with actual data. For ease of reference, this data is collected in the Appendix.

From the open literature data recorded in the Appendix, it is found that

1. The Young's modulus for the glass is 20X larger than that for the film.
2. The tensile strength of the film is 5X larger than that for the glass.
3. A typical thickness of film (0.15 mm) is only 1/50 that of the glass (7.5 mm)

### 5a. Explosive blasts

### Blast: glass window without film

From the data in the Appendix, consider the following situation:

| | |
|---|---|
| Blast overpressure | $(2.8 – 27.6) \times 10^5$ dynes/cm$^2$, |
| Duration | $10^{-2}$ seconds |
| Equal x and y dimensions | |
| Glass thickness | 0.75 cm |
| Glass density | 2.5 g/cc |
| Young's modulus | $6.9 \times 10^{11}$ dynes/cm$^2$ |
| Poisson ratio | 0.23 |

Then eq. [5] gives for the resulting maximum stress at the center of the window:

$$\sigma(\max) \approx (4.3 – 42.3) \times 10^8 \text{ dynes/cm}^2$$

This is to be compared with the maximum tensile strength of the glass:

Tensile strength = $(4.1\text{-}4.5) \times 10^8$ dynes/cm$^2$.

Accordingly, we find that for ordinary blast overpressures of $2.8 \times 10^5$ dynes/cm$^2$, the window is at the limit of withstanding the blast. However, with respect to the government-recommended specification to withstand a pressure of $27.6 \times 10^5$ dynes/cm$^2$, the window stress exceeds the tensile strength by about a factor of ten.

**Blast: glass window plus film**

Next consider the case where the stress induced by the explosion is so large that it exceeds the tensile strength of the glass, and the glass shatters. In that case, only the film can hold the window plus film system together. The relevant parameters for this case are therefore:

| | |
|---|---|
| Blast overpressure | $(2.8 – 27.6) \times 10^5$ dynes/cm$^2$ |
| Duration | $10^{-2}$ seconds |
| Equal x and y dimensions | |
| Glass thickness | 0.75 cm |
| Glass density | 2.5 g/cc |
| Film thickness | 0.015 cm |
| Film Young's modulus | $3.45 \times 10^{10}$ dynes/cm$^2$ |
| Poisson ratio | ~ 0.33 |
| Film tensile strength | $2.08 \times 10^9$ dynes/cm$^2$ |

Inserting these parameters into eq. [5] and using the effective density just derived, we find

$$\sigma(\max) \approx (0.63 – 6.3) \times 10^9 \text{ dynes/cm}^2$$

This is to be compared with the film tensile strength

$$\text{Film tensile strength} \approx 2.08 \times 10^9 \text{ dynes/cm}^2$$

Interestingly, for a normal overpressure of $2.8 \times 10^5$ dynes/cm$^2$, the film tensile strength is about 3X the maximum induced stress, whereas for the government-recommended overpressure limit of $27.6 \times 10^5$ dynes/cm$^2$, the induced stress exceeds the film tensile strength by a factor of about three.

The film has indeed improved the situation.

The maximum induced stress can be decreased by adding more layers of film. Unfortunately, eq. [5] shows that with the effective mass density, the maximum induced stress is only proportional to $h_{film}^{1/2}$. Thus if four layers of film are used, the maximum induced stress is reduced by only a factor of two.

Our equations suggest that the solution for increased blast resistance is to use glass that has been heat treated to obtain a greater tensile strength, in combination with multiple layers of film.

For example, if the heat treated glass has a tensile strength that is larger than that of untreated glass by a factor of three, then that glass could be used with a single film to make a system that would satisfy the government's most stringent case.

**5b. Projectiles**

The relevant equation here is eq. [7].

**Projectiles on glass alone**

Consider the situation described in the Appendix for tempered glass:

| | |
|---|---|
| Breaking stress (60 sec load) | $16.6 \times 10^8$ dyne/cm$^2$ |
| Impact velocity | 1829 cm/s |
| Mass of missile | 5 gm |
| Area of impact | 0.4 cm$^2$ |
| Glass thickness | 0.75 cm |
| Glass density | 2.5 g/cc |
| Young's modulus | $6.9 \times 10^{11}$ dynes/cm$^2$ |
| Poisson ratio | 0.23 |

For these parameters, eq. [G4] gives for the maximum induced stress:

$$\sigma \text{ (max)} \approx 7.25 \times 10^9 \text{ dynes/cm}^2$$

This is to be compared with the tensile strength of the tempered glass:

$$\text{Tensile strength} = 1.7 \times 10^9 \text{ dynes/cm}^2$$

The maximum induced stress exceeds the tensile strength by a factor of 4.3. Accordingly, the projectile would shatter the glass and penetrate.

**Projectiles on glass plus film**

Next suppose that a thin film is added to the glass. For the tempered glass, the tensile strength of $1.7 \times 10^9$ dynes/cm$^2$ is comparable to the tensile strength of the film (e.g. $2.08 \times 10^9$ dynes/cm$^2$). However, the film's Young's modulus is 20X smaller than that of the glass, so the maximum stress developed in the film could be smaller.

To see if this is the case, again consider a situation where the glass has shattered, and the only contribution to the induced moments is that due to the film. As before, the glass now contributes to the problem only through its effect on the mass density:

The relevant parameters are:

| | |
|---|---|
| Glass thickness | 0.75 cm |
| Glass density | 2.5 g/cc |
| Film thickness | 0.015 cm |
| Film Young's modulus | $3.45 \times 10^{10}$ dynes/cm$^2$ |
| Poisson ratio | ~ 0.33 |
| Film tensile strength | $2.08 \times 10^9$ dynes/cm$^2$ |

With all the parameters in eq. [7] now being those of the film – except for the effective mass density, which is given by eq. [12], eq. [7] gives for these parameters:

$$\sigma \text{ (max)} \approx 4.47 \times 10^9 \text{ dynes/cm}^2$$

This is to be compared with the tensile strength of the film:

$$\text{Tensile strength} = 2.08 \times 10^9 \text{ dynes/cm}^2$$

The maximum induced stress in the film is 2.2X the tensile strength of the film, whereas for the glass by itself, the maximum induced stress is 4.3X the tensile strength of the glass.

To summarize, the theoretical predictions give results that are within a factor of five of the data recorded in the Appendix.

## 6. Recommendations

The simple scaling laws and the data comparisons of the previous section give support to the following recommendations:

**For increased blast resistance only:**

1. Use glass that has been heat treated to obtain a greater tensile strength.
2. Additionally strengthen the glass with one or more layers of film.

For example, if the heat treated glass has a tensile strength that is larger than that of untreated glass by a factor of three, then that glass could be used with a single film to make a system that would satisfy the government's most stringent case.

**For both blast and projectile-resistance:**

1. Use a plastic-like material that has a relatively low Young's modulus (like the film material) but that has a thickness similar to a standard glass window.
2. Stiffen by adding layers of tempered glass (with a larger Young's modulus) of comparable or less thickness.

The film and tempered glass would both have tensile strengths of the same order of magnitude, but the lower effective Young's modulus for the system would result in a smaller induced stress.

The foregoing treatment has been somewhat crude: Nonlinear effects have not been taken into account, and no attempt has been made to describe the interesting radial and concentric fracture patterns that can result when a window breaks. Nevertheless, the results are within a factor of at most five of the guidelines in the Appendix, and so it is felt that the resulting simple scaling laws of eqs. [5]-[12] can be useful as a rough analytic guide to designing window systems that are resistant to both blasts and projectiles.

## References

Applied Products , http://www.appliedproducts.co.uk/index.php?cpage=fullstory&article id=90&item type=SEC] (2011)

Architectural Record accessible on line at http://archrecord.construction.com/print.asp? (2006)

Ray E. Bolz and George L. Tuve, eds., **CRC Handbook of Tables for Applied Engineering Science, 2nd Edition.** Boca Raton, Fl: CRC Press, Inc. (1986)

R. Courant and D. Hilbert, **Methods of Mathematical Physics, Volume 1.** New York: Interscience Publishers, p. 192 (1953).)

MI5: Protection against flying glass, accessible at www.mi5.gov.uk/output/Page169.html (2006)

Tempered glass properties at http://www.alumaxbath.com/tech/tgp.htm (2004)

S. Timoshenko, **Theory of Plates and Shells.** New York: McGraw-Hill (1940),

3M Scotchshield™ Ultra Safety and Security Window Films from the 3M website www.3M.com/window/film (2011)

Carl S. Young, **Metrics and Methods for Security Risk Management.** Burlington, MA, Syngress (2010)]

## Appendix

This appendix summarizes typical design guidelines and properties of window glass and films.

**Typical design guidelines for blasts [from the Architectural Record accessible on line at http://archrecord.construction.com/print.asp? (2006)]**

Common blast level: 4 psi overpressure at an impulse level of 28 psi x milliseconds

Enhanced blast level: 10 psi overpressure at an impulse level of 89 psi x milliseconds

Some government agency requirement: 40+psi overpressure for a blast duration of several hundred milliseconds

Note that 1 psi = $6.9 \times 10^4$ dynes/cm$^2$. Accordingly, in cgs units, the above translates to

| | Overpressure (dynes/cm$^2$) | Duration (sec) |
|---|---|---|
| Common | $2.8 \times 10^5$ | $7 \times 10^{-3}$ |
| Enhanced | $6.9 \times 10^5$ | $8.9 \times 10^{-3}$ |

**Window glass properties [from Table 1-91 of the CRC Handbook of Tables for Applied Engineering Science, 2nd Edition, Ed. Ray E. Bolz and George L. Tuve, Boca Raton, Fl: CRC Press, Inc. (1986)]**

Window glass specifications satisfying Federal Specification Standard DD-G-451c

| | |
|---|---|
| Density | 2.5 g/cc |
| Young's modulus | $6.9 \times 10^{11}$ dynes/cm$^2$ |
| Poisson ratio | 0.23 |
| Tensile strength | $4.1\text{-}4.5 \times 10^8$ dynes/cm$^2$ |

**Typical security window film properties [3M Scotchshield™ Ultra Safety and Security Window Films from the 3M website www.3M.com/window/film (2011)]**

| | SCLARL150 | Ultra 400 Series | Ultra 600 |
|---|---|---|---|
| Film thickness | 0.051 mm | 0.1 mm | 0.152 mm |
| Young's modulus | $>3.45 \times 10^{10}$ d/cm$^2$ | $>3.45 \times 10^{10}$ d/cm$^2$ | $>3.45 \times 10^{10}$ d/cm$^2$ |
| Tensile strength | $2.08 \times 10^9$ d/cm$^2$ | $2.08 \times 10^9$ d/cm$^2$ | $2.08 \times 10^9$ d/cm$^2$ |

**Typical recommendations for explosion protection anti-shatter film [from Applied Products, http://www.appliedproducts.co.uk/index.php?cpage=fullstory&article id=90&item type=SEC (2011); See also Carl S. Young, Metrics and Methods for Security Risk Management, Burlington, MA, Syngress (2010)]**

"Polyester film at least 175 microns (0.175 mm) should be used: 300 micron (0.3 mm) film should be considered for panes over 10 square meters or for ground floor windows over 3 square meters."

"The specification can be lowered to at least 100 microns (0.1 mm) if bomb blast net curtains are also to be used."

**Recommendations of the British Security Service MI5 (2006)**

The film specifications that Applied Products gives are those cited in the MI5 recommendations for anti-shatter film in its document for "Protection against flying glass" [www.mi5.gov.uk/output/Page169.html (2006)]

In addition MI5 recommends the use of blast resistant glass (i.e., laminated glass) with the following specifications:

| | |
|---|---|
| Minimum thickness: | 7.5 mm |
| Inclusion of polyvinylbutryal interlayer of min. thickness | 1.5 mm |
| Frame mounting able to withstand | $7x10^4$ dynes/cm$^2$ |

These specifications apply to a window pane with area <2 m$^2$. A 1 square meter window has an increased blast resistance, so that the numbers should be increased by 50% to match the increased resistance.

For larger windows, the recommendation is that the $7x10^4$ dynes/cm$^2$ should not be decreased when designing the accompanying frames.

**Tempered glass properties [http://www.alumaxbath.com/tech/tgp.htm (2004)]**

In the production of regular glass, a molten silica-based mix is cooled slowly under carefully controlled conditions. The slow cooling (annealing) relieves undesirable stresses from the glass. Increased strength can be obtained by heating the annealed glass to a temperature near its softening point and then cooling it rapidly. The resulting heat-treated glass is classified either as "fully tempered" or "heat-strengthened".

Typical breaking stresses and impact velocities for fracture are as follows:

| | Annealed glass | Tempered glass |
|---|---|---|
| Breaking stress (60 sec load) | $4.14x10^8$ dyne/cm$^2$ | $16.6x10^8$ dyne/cm$^2$ |
| Impact velocity (1/4" 5 g missile) | 914 cm/s | 1829 cm/s |

Journal of Physical Security 6(1), 59-72 (2012)

Viewpoint Paper

# National Critical Infrastructure Protection in Serbia: The Role of Private Security

Dusan Davidovic, Zelimir Kesetovic, Ph.D., and Olivera Pavicevic, Ph.D.

## Abstract

This article is an attempt to analyze critical infrastructure protection in Serbia and the role of private security. This is undertaken with an understanding that critical infrastructure protection is quite a new concept in Serbia because the critical infrastructure assets, networks, and security providers were previously those of state companies or public enterprises. By first offering a short history of the development of private security in Serbia in the last two decades, we try to analyze the current situation in Serbian after introducing readers to a European approach to critical infrastructure protection. Adopting the CoESS[1] definition of critical infrastructure, we discuss a previous CoESS white paper on public-private partnerships in critical infrastructure protection. We conclude by trying to identify the main conditions for more intensive and efficient public-private partnerships in the field of critical infrastructure protection and security.

***Key words:*** *critical infrastructure, private security, critical infrastructure protection, European Critical Infrastructure Directive, Serbia, public-private partnerships*

[1] CoESS (Confederation of European Security Services) is a confederation of national associations of private security companies throughout the Europe. Those national associations include 51,000 companies, with more than 1,600,000 employees. As such, CoESS is an umbrella organization for national private security industries, devoted to legalizing, harmonizing, and standardizing private security in Europe. CoESS is a social partner in ongoing social dialogue, while the EC (European Commission) and UNI Europe (syndicate organization) are second and third social partners in social dialog.

## 1 Introduction

In the security-related vocabulary in Serbia, the terms "private security" and "critical infrastructure" are relatively new, especially the latter. The phrase "critical infrastructure" doesn't even exist in the official documents of security strategies and policies, but has been used recently in private security professional circles in Serbia, especially in the ones concerned with projects and activities of CoESS in Serbia and the West Balkans.

The term "national critical infrastructure" should encompass all "state-run companies", i.e., all those companies in Serbia which are still owned by the state (the energy sector, telecommunications, transport, post office etc.). In the mid 1950s, these companies were protected by in-house security, with help from the police, and sometime army security services and intelligence services. From the second half of the 1970s, critical infrastructures, and all other state or public property, were protected by a huge, complex network known as the System of Social Self-Protection. In addition to the in-house security services, that System provided two additional layers of company property protection: inner financial control and workers committee control. Despite the fact that there were three layers of protection/controls, frauds and other losses nevertheless occurred. In comparison with today's figures, however, those losses were minor.

The concept of private security is also new to Serbian security systems. In the past 20 years, the private security sector in Serbia has reached an employment level of more than 30,000 employees (almost the same number as police officers), spread out in less than 200 private security companies, with a yearly business volume of approximately €140 million.

The Serbian private security industry is trying to be fully incorporated in the European private security model, promoted by CoESS in the dialog with UNI Europa and EC. This means that private security in Serbia is striving to (1) harmonize its legislation with common European security legislation; (2) adopt all relevant European standards in private security; and (3) become an active participant in regional projects and policies.

This paper is organized as follows. First we will analyze private security and critical infrastructure issues in Serbia. We will then try to identify the critical aspects of the developing public-private partnership in critical infrastructure security and protection in Serbia and the region.

## 2 Private Security and Critical Infrastructure Protection in Serbia

### 2.1 Private Security in Serbia

Private policing is a relatively new phenomenon in the Serbian internal security system. The country experienced a sudden growth in the number of private security companies at the end of 1992, a development stimulated by the abolition of the Law on Social Self-Protection in 1993. This period signals the beginning of the private security sector in Serbia. From the outset, the development of the private security sector was moving in two directions: (1) towards establishing private agencies that were engaged in protecting "new businessmen", politicians, and celebrities, but also criminals and both former and current members of the secret services; and (2) towards establishing private security companies that inherited the role and jobs of former security services in public companies that were engaged in traditional roles of securing property, people, or businesses (Davidovic, 2009).

In a relatively short period of time (about a decade), the number of employees in the private security sector came close to the number of employees in the police, more than 30,000. This increase in the private security sector is a direct consequence of the change of the state regime following October 5$^{th}$, 2000. The process of privatization, and the arrival of foreign companies in the Serbian market, has led to an increase in the quality and quantity of private security.

This rise in the Serbian private security industry is confirmed by data indicating that the annual gross income of private security companies increased from €10 million in 2001 to approximately €26 million in 2003 and to €140 million in 2010 (according to official data from the NBS Solvency Centre). Investments by owners of private security companies have

tended to be directed towards new security technologies and equipment, rather than employee training and education.

Since the beginning of the development of the private security sector, there has been a chronic absence of legal regulation. Despite the fact that several pieces of legislation indirectly regulate the framework and the character of the private security field, a separate law on private security would largely prevent the serious problems that the security field faces in Serbia. These problems represent the main focus of this paper.

In an analytical sense, the general challenge that the private security sector of Serbia is facing is the ability to shape, build, and harmonise itself with the European model of private policing. Specific problems include:

1. The absence of an appropriate and contemporary categorical apparatus in the field of internal security, which results from the fact that in Serbia there is no clearly formulated national security concept based primarily on prevention (rather than repression). The course of historical change suggests that the social environment is increasingly becoming dominated by private entities.
2. This absence of a conceptual apparatus negates the possibility of an analytic framework from which to engage with critical opinion, conceptualization, and strategic planning.
3. There is a lack of legislation with which to regulate the many problems (or at least ill-defined issues) that occur in the private security sector. Examples include abuse of private surveillance systems by private investigators/detectives or other private security practitioners, the lack of regulation for tendering private security services, the lack of systematic training and education of security employees, problems with licensing of companies and employees in the security sector, the protection of employees' rights, and illegal competition in the security services market.

There is a serious lack of partnership between the private and state security sectors, which is a key precondition for ensuring the security and safety of citizens, the local community, and society in general. This is aggravated by 2 factors. Firstly, the governing

model of internal security in Serbia is one of state-centralization. Secondly, there is evidence of a persistent stereotype that holds that the police are the only legitimate provider of security in society (Kesetovic Z., Davidovic D. 2009).

A lack of communication and cooperation between public and private security sectors suggests that the Ministry of the Interior (MoI) and Serbian authorities are torn between competing demands to re-define and organize modern policing, on the one hand, and demands to preserve the status quo, on the other.

There is a lack of any concept of crime prevention at the national level, and therefore a lack of any vision about the place and the role of the private sector in prevention. Indeed, this raises the issue of the extent to which we can even talk about private policing in Serbia at all. If we strictly adhere to the definition of policing as a social concept that involves a wide circle of social factors involved in the maintenance of social order, then we can say that Serbia remains in the initial stages of creating conditions for the establishment of a private policing model.

The concept of policing actually represents a socialization[2] of the function of security. The concept has historical precedent within Serbia, and for two decades we have witnessed the system of social self-protection, the process of socializing the function of security against a strong ideological backdrop. Nevertheless, the huge social experience derived from the practice of social self-protection could and should be used in organizing the emergent concept of modern policing in Serbia.

The private security industry, despite the presence of unresolved problems, is entirely ready to integrate itself into such a concept. These problems can be easily and efficiently removed through the application of 4 basic principles: (1) the principle of legalization; (2) the principle of professionalization; (3) the principle of standardization; and (4) the principle of europeization.

The private security sector in Serbia is undeniably a reality as is the public/state sector. What has yet to become a reality is communication between the two sectors, and cooperation on the general concept of crime prevention, the removal of the threat of crime,

[2] By the term "socialization" we understand a process of becoming public, i.e. common thing, common duty, common responsibility

and the elimination of the fear of crime that we have suffered for the past decade. However, at the same time, the private security sector represents an existing force that, with the expansion of its activities, will gradually increase in power, and subsequently find itself in a different negotiating position. Meanwhile, the relinquishing of traditional jobs and authority of the state monopoly also represents a measure of democratization of society. Judging by the present situation, and the activities carried out by the state security sector and the authority it continues to hold, the monopoly of state power embodied in the Ministry of Interior (MoI) still exists.

Perhaps it would be more precise to say that a large discrepancy exists between the proclaimed reform initiative of the MoI and what has actually been achieved in that sphere, and the extent of adjustment to market laws and private security sector models of development. Even though the lack of legal regulation in this field suited many (generally smaller) private security companies for quite some time, the past five years have seen the entire private sector publicly insist on the necessity of passing legislation.

After failing to prove receptive to such requests, there has been a growing awareness of the fact that private security is becoming international, and that leading private companies are establishing associations and are on the threshold of being accepted to CoESS (the Confederation of European Security Services). Central to this was a desire to standardize and professionalize their practice according to the European model and its associated market. There are many examples of attempts by private security companies to enhance the professional level of their personnel, by contracting with renowned scientific and qualified institutions, by investing substantial funds in state-of-the-art equipment, and by establishing cooperation with other companies in the region.

What we thus have is an absurd situation in which the social practice of private policing comes before social regulation in terms of norms and legislation. The majority of private security companies have certified their work according to ISO standards for commercial practice. Even though this is not a standard that refers solely to the field of security, its use indicates how seriously and professionally private security companies wish to do their job.

## 2.2 Critical infrastructure Security and Protection in Serbia

### 2.2.1 European Approach

We will consider "critical infrastructure" in the way CoESS did it in its white paper on critical infrastructure security and protection (CoESS, 2010), namely that critical infrastructure encompasses physical assets, networks, and organizations whose disruption or disabling would cause severe, lasting damage to social and economic life. Various national authorities have drawn up broadly similar lists of economic sectors which are covered by this definition; they generally include energy, water and food supplies, waste management, key transport networks (major airports and rail interchanges), financial institutions and cash supply, health services, and state emergency response organizations.

The European Union has recently started dealing with the problem of critical infrastructure protection. This increased emphasis on the protection of critical infrastructure is articulated in the European Critical Infrastructure Directive (Council of Europe 2008) which focuses on so-called "European" critical infrastructure (ECI)—assets or systems whose disruption would have a major impact on at least two EU Member States, or a Member State other than the one in which the asset or system is located (CoESS, 2010).

The Directive mandates Member States to identify all such infrastructure, ensure a risk assessment is carried out for all its elements, and ensure an Operator Security Plan (OSP) is drawn up. The broad headings which must be included in each plan are set out in the Directive. Each Member State must check that its ECI elements each have an OSP. If any ECI operator has failed to draw up such a plan, the Member State may take "any measures deemed appropriate" to ensure it does so.

Member States must report every two years to the European Commission "generic data on a summary basis on the types of risks, threats and vulnerabilities encountered per ECI sector" (CoESS, 2010).

This Directive surely represents a useful tool in the strategic battle for security and safety of countries and their citizens on Europe's territory. We must, however, ask ourselves what's happening with the countries that are neither members nor candidates for EU membership. A huge number of critical infrastructures are dominantly of either national or local character and as such are outside the purview of ECI. The fact that any attacks on critical

infrastructures, even if they are of a local nature, can seriously jeopardize social and economic elements of a nation's life, or several of them, the question arises whether this Directive has an integral European character, or whether it is a consistent system of critical infrastructure protection of EU members alone.

This question is inevitably asked by EU country candidates, and even more often by the countries that are about to become candidates. In many of these countries, the term "critical infrastructure", as is the case in Serbia, does not appear in security policies. In other countries, even in those that have recently become EU members, the remains of old security policies and practices, and unfinished reforms of security structures/systems play an important role, and these countries may be insufficiently flexible and unprepared to adequately integrate themselves into the global European security environment.

In that sense it could be productive to take into consideration the possibilities of applying the ECI Directive to the West Balkans. Firstly, because of the fact that the ways in which critical infrastructures have been secured and protected in many European countries vary from 100% by state authorities (police, military, specialist protective services), through a mixture of state in-house security and private security service, up to fully contracted private security. A similar situation exists in Western Balkan countries.

Secondly, because experience and good practices already exist in EU countries, these could be leveraged to improve practices in the Western Balkan region.

Thirdly, security and protection of critical infrastructure (in addition to other areas) are increasingly based on Public Private Partnership (PPP). This model of security policy is not very familiar to Western Balkans countries or, or at least this model is just beginning to be adapted. Securing and protecting critical infrastructure is one of the most suitable areas for public-private partnerships, given their often public (national or local) character, which is translated in public ownership or public management or public objective. It is also undoubtedly a development in Europe in general that more and more sectors and assets are taken away from public security to the benefit of the private security sector (CoESS, 2010).

From the following examples, which are quoted by the aforementioned white paper (CoESS 2010), it should be clear that it would be important and useful if the ECI Directive would expand to West Balkan countries.

### 2.2.2 Best Practices in PPP for Protecting Critical Infrastructure

In the aforementioned white paper, CoESS recognized some vivid examples of efficient public-private partnership in protecting critical infrastructure.

Project Griffin in the United Kingdom, for example, was established in 1994 by the City of London police. It was meant to deal with security in the financial district of London, which has been targeted several times by terrorists. This project consists of four key activities:

- Awareness training for private security officers, provided by the local police. The focus was on how to recognize, respond to, and report suspicious activity such as terrorist surveillance of potential targets.
- Online refresher courses which maintained participants` interest and skills and enabled formal accreditation.
- Regular communication between police and security officers, either by conference call, SMS, message, or e-mail, to ensure current intelligence and incident reports are disseminated in a timely manner
- Emergency deployments: private security officers who have undergone Griffin training may be used by police to support them in responding to incidents, for instance in establishing and manning cordons.

Project Griffin has been rolled out to approximately half the police forces in the UK as well as to ports and airports. It has also attracted attention in the USA, Australia and Singapore (CoESS, 2010).

Another example is the German cities in which private security companies have come together with the local police to pool information and share it with the police In these projects, mobile patrols by private security companies, travelling between costumers sites, may spot suspicious persons or vehicles, or may witness possible unlawful activity. The officers transmit this to their company operations center, which then passes it on to the local police for assessment and possible further action. This public-private cooperation has proven to be highly effective, and is very welcomed by the German police forces. Through incorporating private mobile patrols the number of “surveillance vehicles” on the street each night has been more than doubled (in some cases even tripled) in comparison to the number

of police vehicles patrolling these cities. In one German city, Düsseldorf, for instance, the scheme has led to more than 500 reports of suspicious activity including 12 burglaries and one fire.

A third example of an effective public-private partnership comes from Spain where police recognise that private security officers are a valuable resource. All contracts signed between private security companies and their customers must be registered with the police, including details of the numbers of staff involved and services provided. The police have also established a 24-hour telephone number to enable them to communicate rapidly with the private security industry (CoESS, 2010).

These case studies clearly demonstrate that well-defined, well-managed and well-monitored public-private partnerships are efficient, effective and, increase the security of critical infrastructure.

CoESS researches concluded that, in order to be successful, these partnerships must comply with certain criteria. These include an open dialogue between responsible public authorities and private security providers, clear instructions regarding the role of each partner, a clear legal or contractual framework, regular evaluation, and necessary corrections and improvements when and where needed.

### 2.2.3 The Case of Serbia

Most of the critical infrastructure in Serbia is protected by former in-house (state) security services. During the 90's period of privatization, these security services became separate companies which now offer services to customers like any other private security company on the private security market. But for now, they primarily protect only public companies, that is, they protect the critical infrastructure from which they originated.

This is particularly the case for the sectors of energy, water-management, post office, telecommunications, and railways. Other critical infrastructure such as the health sector, water supply, river ports, airports etc. are protected by private security companies, usually in a mixture with in-house security services.

In our view, the key problems in critical infrastructure protection in Serbia are: (1) cases of severe economic crime within critical infrastructure; (2) absence of public-private partnerships in protecting critical infrastructure; and (3) dramatically politicized management.

Speaking of the first of the aforementioned problems, it turned out that companies which are important and vital for the country and society are the favourite prey of "criminals protected by the state". A recent investigation of crime committed during 8 years in the huge complex of the thermal-power plant Kolubara, by the management and managing board members, tentatively shows a paradoxical situation in that many critical infrastructures in Serbia are primarily endangered from the inside and not from the outside. The dossier consisting of more than 30,000 pages regarding the crime committed in this thermal power plant that caused the damaged worth more than €250 million, tells a lot about the size and severity of the problem.

The second problem, the absence of PPP, is a chronic disease of internal security in Serbia. Research carried out in 1986 (Davidovic, D. 1993) by the Institute for Crime and Sociology Related Research showed that the partnership between the police and security service in public companies almost didn't exist. This can be explained by the strong stereotypes about the omnipotence of the police in security-related activities, but also by the low level of democracy in Serbian society.

The third problem is the joint problem of the majority of societies in transition. Such societies experience all the negative consequences of chaotic privatizations carried out in ways that tend to line the pockets of political, criminal, and economic elite from the former socialist governance. Indeed, critical infrastructure security in Serbia that hasn't been privatized has become the prey of political parties that take considerable funds from these rich companies to finance their programmes and campaigns. That kind of management always has to ask its party top officials in the first place whether it may introduce a novelty/change in the company management, especially if those changes regard security policy within critical infrastructure.

## 3. Conclusion

The role of private security in Serbia is continuing to expand. There are three main reasons for this. After 18 years, private security in Serbia has finally become legalized; a special law on private security is in the process of being adopted. Also, the Serbian Association of Private Security Companies and the Association for Private Security at the Serbian Chamber of Commerce are raising awareness of private security, and the need for professionalization and standardization. Finally, CoESS is providing important assistance in the processes of preparing Serbian private security to enter a European model.

Private security in critical infrastructure protection has clearly not reached its full potential in Serbia. Best practices discussed in the CoESS white paper that we quoted so much in this article seems like a distant goal for private security in Serbia. Public-private partnerships in UK, Germany, and other countries could be very useful examples of practicing PPP not just for Serbian, but for the other countries in the region as well

In our view, the critical infrastructure protection strategy given in the ECI Directive, the coordination with private security in EU done by the CoESS, and the proscribed guidelines for enforcing public private partnerships, also by CoESS, must become “homework” for all key actors in the field of security. This include responsible decision makers (governments, politicians), owners and operators of critical infrastructure, and the private security services industry as a whole.

## 4. Acknowledgments

We are grateful to the Editor and anonymous reviewers for their suggestions and assistance with this paper.

## References

Davidovic, D. (2009). Public-Private Security Sector Partnerships in Serbia- Problems and future development . *Varstvoslovje 2.* , 345-351.

Kešetović, Ž., Davidović, D., (2007) Policing in Serbia – Challenges and Developments in *Policing in emerging democracies - Critical reflections*, Meško, G. and Dobovšek B. (eds.) Ljubljana:Faculty of Criminal Justice and Security, 2007 pp. 79-100.

Confederation of European Security Services (CoESS) (2010). *Critical Infrastructure Security and Protection- The Private –Public Opportunity.* Paper and Guidelines by CoESS.

Davidovic, D. (1993) Self-Management Policing in Yugoslavia.. In Findley M. And Zvekic U.: *Alternative Policing Styles.* UNICRI, Kluwer Law and Taxation Publisher, Deventer, The Netherlands 1993.

## About the Authors

**Dušan Davidović**, Sociologist, is an independent researcher at the Institute for Criminological and Sociological Research, and the Director of the Crime Prevention Center. From 2003-2006, Professor in Sociology at the Police College in Belgrade. Author of many articles published in domestic and foreign journals; author of numerous papers presented at national and international conferences; Managing Director of various training courses for private security personel; one of the founders of Specialist Studies for security managers at the Faculty of Civil Defence. President of the National Commision of Private Security Companies in Serbia, member of CoESS.

**Zelimir Kesetovic,** Ph.D. Political scientist and Associate Professor at the Faculty of Security Studies (Crisis Management). From 2000-2005, Professor at the Police College (Sociology) and Head of the Research & Development Unit. Member of the Think Tank for the police reform in Serbia. Expert consultant of the OSCE for the following projects: Police-Media Relations and Policing Diversity. Author of several monographs and a number of papers presented at national and international conferences and published in domestic and international journals.

**Olivera Pavicevic**, Ph.D. Political Scientist. Scientific Assistant at the Institute for Criminological and Sociological Research in Belgrade. Author of many articles published in domestic and foreign journals. Actively participating in all research at the Institute.

# Assessing the Performance of Corporate Private Security Organizations in Crime Prevention in Lagos State, Nigeria

Oluwakemi Omotoso, Ph.D. and Adeyinka A. Aderinto, Ph.D.
Department of Sociology, University of Ibadan, Ibadan, Nigeria
Email: aderinto@yahoo.com

## Abstract

Corporate private security organizations have become more visible in crime prevention because of the rise in crime rate due to mass urbanization and population expansion. In spite of their increasing importance, an assessment of their performance has not been empirically investigated. This study, therefore, assessed the performance of the CPSOs in crime prevention in Lagos State. Data were obtained using a combination of a questionnaire and In-depth Interview (IDI) methods. Copies of the questionnaire were administered to 1,200 respondents in gated neighborhoods in four Local Government Areas (LGAs) of Lagos State namely, Island, Shomolu, Ikeja and Amuwo/Odofin LGAs. Thirty IDIs were conducted with members of staff and management of private companies, corporate guards, and proprietors of CPSOs. Findings revealed that many residents (46.5%) perceived the performance of corporate guards to be fairly effective, 18.7% perceived them to be ineffective and 34% of the respondents were indifferent. Overall, CPSOs were perceived to be relevant in crime prevention in Lagos State.

## Introduction and statement of the problem

The significance of security to mankind cannot be over-emphasized as the socio-economic structure of any society or organization depends on the security system available in such society or organization (Oyegoke, 2003). Hence, human beings and societies since the beginning of time have developed measures to safeguard themselves and their properties against threat. Some of these measures predate the institutionalization of the public police and other uniformed institutions. Thus the term: public police, as an institutional noun can be distinguished from policing as an atomized verb, in which every individual shares both roles and benefits. As a result, while the state remains dominant in the security sector in the present age, it is not the only significant actor (Odinkalu, 2004). The idea that people have a right to protect themselves against any threat has existed since time immemorial. The

exercise of this right was prior to the idea that government efforts for that purpose will materialize in form of public police (Dempsey, 2008).

No government has the wherewithal to provide one hundred percent security for her people, hence the need for the corporate private security providers (corporate providers) to complement efforts of state actors in crime prevention (Ekhomu, 2004). Mayah (2003) opines that this expansion in security needs gave rise to Corporate Private Security Organisations (CPSOs), first in the developed world and later in the developing world. These needs might also include citizens' fear of crime, and awareness that the public police cannot effectively control crime by themselves. Therefore, this mandates greater co-operation with the private sector and its resources to jointly forge a partnership for crime prevention and reduction. In addition, as Fischer and Green ( 2004) assert, the ingenious use of corporate private security's human resources and technology may be the one practical option left for crime prevention in communities.

Crime prevention has been defined as a pattern of attitudes and behaviors directed both at reducing the menace of crime and at enhancing the sense of safety and security to create a society where crime cannot thrive. Crime prevention approaches have grown out of different traditions across the world. The tradition normally adopted by corporate providers is the Australian Model. This model explains situational crime prevention as a method to reduce crime through management, design, and expansion of the physical environment by reducing the chances of committing crime. Examples include installation of surveillance cameras in public places, guards patrolling, man-guarding and access control, and so on (Dambazau, 2007). In essence, most corporate private security policies are aimed at reducing the risk of crime by increasing the risks to offenders (Button and George, 1998). Corporate private security personnel (corporate personnel) are those self-employed individuals and privately funded business entities and organizations providing security-related services to specific clientele for a fee, for the individual or entity that retains or employs them, or for themselves in order to protect their persons, private properties or interests from various hazards (Bohm and Haley, 2002).

The security framework is much more sophisticated today than in the past and the context and operations of policing are changing worldwide (Aremu, 2009). No government has found it solely able to provide security for its people because of the importance of security in the development of any nation, and the complexities therein. This is especially the case in Nigeria, with rising crime and the inadequacy of the public police. Recognizing these problems, the Ministry of Police Affairs has made several efforts aimed at invigorating the Nigeria Police by re-structuring, re-equipping, and strengthening the workforce (Jemibewon, 2000). Despite all these efforts, the Nigeria Police cannot always prevent crime as an important part of proactive crime prevention because of inadequate manpower, advanced technological means, and programmatic means for fear reduction. Therefore, the CPSOs who do possess all these qualities are in a very strong position to assist the Nigeria Police. Thus, the vacuum created by the inadequacy of state actors both in manpower and technology to provide security will certainly be filled by the CPSOs (Ekhomu, 2004).

The private business sector is the biggest employer of the CPSOs in Nigeria because many private companies are employing private security providers (most especially the corporate guards) to serve the needs of the business sector for industrial security, which the public police cannot adequately provide. The employers of these corporate guards have differing perceptions of the performance of the guards employed. Members of the public also come in contact with the corporate guards especially in private companies and on private properties. The corporate guards are often the interface between their clients and members of the public in private companies and on private properties. Members of the public can also be expected to have varying perceptions of these private guards and the security services they provide. In spite of all these realizations, and the growing demand for CPSOs, few studies have been carried out on CPSOs in Nigeria. The studies that have been conducted have totally neglected assessing the performance of CPSOs in crime prevention in Lagos State. Addressing this gap constitutes the central concern of this study.

## Literature review

The private security industry has a long history in Nigeria (Oxford Business Group, 2010). The CPSOs in Nigeria complement the activities of the public police by providing private security mainly to the private business sector and members of the public. With the advent of CPSOs more than twenty years ago, the industry has continued to play an important role in crime and loss prevention (Mayah, 2003). The Minister of Interior, Captain Emmanuel Iheanacho, observed that the country's size, its growing population, ethnic diversity, and socio-political and economic dynamics have made the services of the private companies unavoidable in the provision of sufficient security for the citizens. As in all civilized societies worldwide, the arduous task of preserving law and order is better complemented by the services of well-trained and disciplined corporate guards (*Compass*, 2010). The Lagos State Commandant of the NSCDC, Mr. Nathaniel Ubong, tasked the CPSOs on crime in Lagos State when he addressed corporate providers recently in Lagos and he confirmed that the CPSOs are crucial to a crime-free society (*Daily Trust,* 2007).

It is difficult to date the beginning of CPSOs in Nigeria, as there are different dates given by different sources. The CPSOs have been linked to the work of a man named Victor Vanni in the early 1970s (Cleen, 2001). However, Ekhomu (2004) posits that the CPSOs had their beginnings in 1965, when Alhaji Mumuni founded the Nigerian Security and Investigations Company. Some of the CPSOs founded in this era include: Nigerian Investigation and Safety Company, founded in 1967; Omo Security Services, which started operations in 1971; Metropolitan Guards, and Arksego (Nigeria) Limited, founded in 1980 (Roberts, 2003). The Nigerian Security and Civil Defence Corp ( NSCDC) representative in Lagos State, Mr Emmanuel Okeh, commented that about 80 CPSOs were registered in the last two years (*Vanguard,* 2008). Nineteen CPSOs in Abuja were registered by NSCDC for full operations across the country (*Daily Trust,* 2010). There are over 350 CPSOs registered in Lagos State and an estimated 1,000 CPSOs registered nationwide (Oxford Business Group, 2010). Corporate providers are highly noticeable around the country, guarding businesses, homes and neighborhoods and advising transnational companies and embassies on risks and dangers to their assets and employees (Abrahamsen and Williams, 2005). Indeed, "The entire

civil security system of corporate Nigeria is in the hands of private security companies" (Ekhomu, 2004:139).

The private business sector is the main client of CPSOs in Nigeria. Examples of such include the Non-Governmental Organisations (NGOs), banking institutions, oil companies and embassies. At times, the CPSOs protect public facilities such as oil installations, international and state airports, and national stadiums (Roberts, 2003). The CPSOs in Nigeria protect public facilities, such as the National Stadium Surulere, Murtala Mohammed International Airport in Lagos State, and Osubi Airport in Warri, Delta State (Ekhomu, 2004). The public sector has also begun to employ corporate guards to reduce pressure on an over-stretched public police, with a selection of airports and ministries now collaborating with the CPSOs (Oxford Business Group, 2010). Many oil companies, banking institutions, embassies and other transnational firms have a triple security structure in place, relying on a combination of proprietary security (otherwise known as in-house security), the public police, as well as the CPSOs. This combination provides multiple business prospects for the private companies (Abrahamsen and Williams, 2006).

Increasingly, oil companies are supplementing their use of public security services with the services of the CPSOs. Many oil companies employ a combination of the public police and CPSOs for guarding services. There is also an expanding use of security consultants from international and foreign CPSOs, such as Control Risks International, ArmorGroup, and Group4Securicor. These CPSOs are entrenched in the companies' security structures in the private business sector (Abrahamsen and Williams, 2005). Next (2010) notes that the Niger Delta, the source of crude oil in Nigeria, has many foreign CPSOs providing private security services for clients in the oil and gas industry. The foreign CPSOs provide in the Niger Delta (as elsewhere) private security services for personnel and property to prevent insurgency, piracy, and terrorism acts. The Niger Delta, in particular, has become infamous for piracy, kidnappings, and sabotage of oil installations. Prominent among the foreign CPSOs in the Niger Delta are Control Risks International, Erinys International, ArmorGroup, Aegis Defence System, and Northbridge Service Group.

Bamgbose (2003) and Mayah (2003) claim that there is an increasing professionalism in the private security industry because of the increasing presence of ex-military men and former public police personnel in the industry. The position of the industry in Nigeria has also brightened with the employment of graduates and post-graduate degree holders. The industry in Nigeria is generally undergoing increasing professionalism with several leading companies incorporating the use of technology and equipment such as satellite tracking, radio alarms, panic buttons, and armored vehicles. Furthermore, there is an increasing move towards offering integrated risk analysis and consultancy services, as CPSOs seek to protect their employers and their assets in an increasingly insecure environment (Abrahamsen and Williams, 2005). The increased professionalism is being driven by a perceived need for a code of ethics and for credentials, including education and training, experience, and membership in professional societies (Mayah, 2003). The drive towards professionalism is also noticeable in the rapid growth of active security professional organizations and associations (Fischer and Green, 2004).

With the enactment of the NSCDC Act by the National Assembly in June 2003, the implementation of private guards matters is now policed, monitored, and reported upon by the NSCDC to ascertain compliance or otherwise (*NSCDC,* 2005). To inject some sanity into the private security industry, nine CPSOs were recently shut down in Ibadan by the NSCDC. According to the Public Relations Officer of the Oyo State Command of NSCDC, the CPSOs were shut down because they failed to comply with the rules for private guards licensing (*Tribune,* 2006). The NSCDC also went on an exercise in 2007 to cleanse the industry in the country. In the process, 500 CPSOs that did not meet the standards set by NSCDC were closed down. Some of these CPSOs were formed by retired military officers who set up such security companies without meeting legal requirements (*Vanguard,* 2008). Commandant-General of the NSCDC, Dr. Ade Abolurin, admonished CPSOs to operate within the law and warned registered CPSOs in the country to discontinue having a foreigner as their director or board member, threatening to withdraw the license of operations of any CPSO found guilty (*Vanguard,* 2010). The strategy of the Federal Government of Nigeria is to have the CPSOs complement the efforts of the public police in crime prevention (Ekhomu, 2004). In spite of

their unarmed status, the CPSOs exercise a fundamental impact on the security situation in Nigeria through the operation of public-private networks (Abrahamsen and Williams, 2006).

## Methodology

### Study sites

Four local government areas (LGAs) in Lagos State, namely Island Local Government, Shomolu Local Government, Ikeja Local Government and Amuwo/Odofin Local Government Area, were purposively selected for this study because they have the highest concentration of corporate guards in gated neighborhoods within residential areas. The study population consisted of different categories of members of the public who are users of services provided by the private security industry.

In Nigeria, as in other parts of the world, the private business sector is one of the major users (consumers) of private security industry. Banking institutions, telecommunications companies, and eateries in the private business sector were selected for this study because they principally make use of the services of the CPSOs. The members of staff and the management staff of the private companies constitute the primary users of the private security industry. Members of the public who are the residents of the gated neighborhoods in the residential areas in the four chosen LGAs were also interviewed.

### Sample size and sampling method

Five private companies were chosen randomly from the headquarters of private security companies on different streets on Victoria Island. One corporate company was chosen from the telecommunications and eateries sectors, and three banks were selected for interviews. For each of these chosen private companies, the manager in charge of security was purposively interviewed. A member of staff of the corporate company was also randomly sampled. All the selected members of staff and management of the private companies were interviewed in depth.

Copies of the questionnaire were administered on 1200 members of the public. They were chosen using the systematic random sampling from the selected four LGAs in the three senatorial districts in Lagos State. Three hundred respondents were drawn from each of the headquarters of the four LGAs. In each headquarters, two communities were randomly chosen. In each community, six streets were randomly chosen. On each street, twenty-five households were sampled with systematic random sampling. An adult male and an adult female who had lived on that street for at least a year were alternated in the twenty-five households on each street

Data collection instruments

The study utilized both quantitative and qualitative instruments. The quantitative instrument was the questionnaire. The questionnaire consisted of both open-ended and close-ended questions with two sections. Section A consisted of the socio-demographic characteristics, such as sex, age, language, educational qualification, religious affiliation, marital status, ethnic group, occupation and income of each respondent. Section B contained questions to elicit responses from members of the public about their perceptions of the CPSOs in crime prevention in Lagos State.

The qualitative instruments used in the study were the in-depth interview and the key-informant interview. Two different interview guides for the in-depth interview were structured to elicit information about the perceptions of the members of staff and management of the private companies. The two types of qualitative interview techniques provided relevant information to achieve the objectives of the study. It also allowed the interviewer to modify the questions according to the mood of the interviewee, obtain detailed responses, and observe the non-verbal communication cues, which enriched the quality of the response.

Secondary data were collected from seminar and workshop papers and all other available publications on CPSOs globally and locally. Official and public records from governmental agencies, such as the NSCDC and the National Population Commission (NPC),

were also very valuable to the study. Data were also gathered from publications and records of the SSPN, an umbrella association for the CPSOs.

## Findings

Engagement and performance of the CPSOs

All the respondents in the qualitative interviews claimed that the employment of CPSOs by the private companies involves a lot of processes. There are checks on the backgrounds of the CPSOs to see if they are licensed and registered. The respondents also confirmed that investigations are indeed carried out on corporate guard training. They further affirmed that the CPSOs that are recruited must have industrial experience and must also have a very good coverage especially in Lagos State. The respondents also claimed that there is no known relationship between the CPSOs and the management except one respondent who maintained that the CPSO belongs to the deputy chairman of the bank.

One respondent responded as follows:

> Yes, we do carry out some security or information checks on the CPSO we want to employ. The CPSO must be registered and licensed. It must have a good coverage. It must also have industrial experience in banks or other corporate bodies. We also look at the prospective CPSOs' management sector to see how organized they are. We also investigate that they are doing well before they are recommended. The recommended ones then pass through a competitive bid to prove themselves. There is no known relationship between the management or any member of staff of the company and the CPSO. MALE IDI/Security Manager/Island LGA

The respondents who were the security managers in the private companies confirmed that the employment of the corporate guards has been cost effective. Most respondents in the qualitative interviews claimed that the cost effectiveness has been in terms of risk transfer and low costs of administration. The extent of risk transfer is that the CPSO (who is the employer) is liable for the actions of the corporate guards as long as they are committed in the course of the guards' employment. The CPSO will be held liable for the loss of property from the premises of the corporate company when such loss is directly or indirectly attributable to

the negligence of the corporate guards. A master is vicariously liable for the tort committed by his servant. It is of no consequence whether the guard carried out his duty in an unlawful manner (Ozekhome, 2003; Oyakhilome, 2003). Consequently the CPSO being the employer and in this case, the master of the corporate guards, would be held liable for any action committed or omitted by the guard.

Another respondent commented that:

> The employment of the corporate guards has been cost effective in terms of finances because I pay my in-house member of staff N70,000 per month and the corporate guard earns N35,000. The employment of the guards has also been cost effective in term of administrative cost of training the guards. Also, there is the issue of risk transfer because if there is any problem, the risk is directly transferred to the CPSO. If the corporate guards steal anything, someone will be held responsible, unlike if they are members of staff. So, it has been cost effective, not only in monetary terms, but also in administrative and risk management.
> MALE IDI/Security Manager/Island LGA

In the words of another respondent:

> The employment of the CPSO has been cost effective in the sense that the corporate guards' job is strictly security. If we start having in-house security to do that job, the in-house people you are getting may not be professional security men. They will see themselves as bankers. So it is been cost-effective in terms of professionalism and also financial.
> MALE IDI/ Security Manager/ Island LGA

The respondents were also asked to comment on the safety of their neighborhoods with the employment of the corporate guards. The results are shown in table 1. Many of the respondents (54%) stated that they feel safe with the employment of the corporate guards in the neighborhoods, while 23.3% stated that the employment of the corporate guards has made no security difference to them. Close to 21% did not respond, and 1.5% claimed that they do not know the security situation of their neighborhoods**.** Results further revealed that the perceptions of the respondents regarding the safety of their neighborhoods with the employment of the corporate guards are significantly related ($\chi^2 = 183.41$, $p < 0.05$) to the respondents' choices about the continued employment of the corporate guards in the

neighborhoods, as shown in table 2. Most of the respondents (96.9 %) who claimed that they feel safe with the employment of the corporate guards in their neighborhoods, agreed that the corporate guards should continue to be employed in their neighborhoods.

The respondents were asked to rate their general perceptions whenever they come in contact with corporate guards. As shown in table 1, about 43% of the respondents declared that they always perceive corporate guards as a means of fear reduction. Very few respondents (4%) declared that they always have a sense of safety anytime they come in contact with corporate guards, while 37.2% declared that they are indifferent anytime they come in contact with corporate guards.

Respondents were further asked to comment on the general performance of corporate guards in crime prevention. Close to 47% of the respondents perceived corporate guards to be fairly effective, while 18.7% and 34%, respectively, perceived corporate guards not to be effective and as making no difference in security provision.

The respondents' perceptions of the safety of their neighborhoods with the employment of the corporate guards are significantly related ($\chi^2 = 381.32$; $p < 0.05$) to the respondents' perceptions of the general performance of corporate guards, as shown in table 3. Close to 80% of the respondents who thought their neighborhoods are safe with the employment of the corporate guards, stated that the general performance of corporate guards is fairly effective.

**Table 1: Perceptions of members of the public of corporate guards in crime prevention**

| **Opinions of safety of neighborhoods** | N | % |
|---|---|---|
| Very safe | 8 | 0.7 |
| Safe | 648 | 54.0 |
| No difference | 280 | 23.3 |
| Don't know | 18 | 1.5 |
| No response | 246 | 20.5 |
| **General perceptions of guards** | | |
| Sense of safety | 548 | 4.0 |
| Fear reduction | 518 | 43.1 |
| Incapable of controlling crime | 174 | 14.5 |
| Indifference | 446 | 37.2 |
| Intrusion | 14 | 1.2 |
| **General performance of guards** | | |
| Very effective | 6 | 0.5 |
| Fairly effective | 558 | 46.5 |
| Not effective | 224 | 18.7 |
| No difference | 408 | 34.0 |
| No response | 4 | 0.3 |
| **Whether guards play important role(s) in national security** | | |
| Yes | 1106 | 92.2 |
| No | 94 | 7.8 |
| **Guards' role(s) in national security** | | |
| Crime prevention/safety | 346 | 28.8 |
| CPSOs complement the public police | 294 | 24.5 |
| Create jobs | 660 | 55.0 |
| Provide private security services | 510 | 42.5 |
| Threat if guards are not well trained | 58 | 4.8 |
| Insecurity if guards' background are not cross-checked | 40 | 3.3 |

**Table 2: Relationship between perceived safety of the neighborhoods and continued employment of the guards**

| Perceived safety of the neighborhood | Continue employment of the guards? | |
|---|---|---|
| | *Yes* | *No* |
| Safe | 96.9% (634) | 3.1% (20) |
| No Difference | 47.1% (132) | 52.9% (148) |
| Don't Know | 22.2% (4) | 77.8% (14) |

**Table 3: Relationship between perceived safety of the neighborhoods and general performance of guards in crime prevention**

| Perceived safety of the neighborhood | General performance of guards in crime prevention | | |
|---|---|---|---|
| | Fairly Effective | Not Effective | No Difference |
| Safe | 79.2% (518) | 6.7% (44) | 14.1% (92) |
| No Difference | 6.5% (18) | 37.1% (104) | 56.4% (158) |
| Don't Know | 11.1% (2) | 33.3% (6) | 55.6% (10) |

The findings from the quantitative data, however, differ from the findings generated from the qualitative data.

A respondent asserted that:

> The services of the private security company have improved a lot. The kind of problems we were having before have stopped. The corporate guards help to complement public police effort…… They alert the police if there is going to be any trouble and so the criminals keep away. It is like we assess the job. In security generally, what we call effective today might be ineffective tomorrow. As crime is growing, they are there to manage it, not to eliminate it. However, when incompetence is noticed, it is either the CPSO or the particular corporate guard is sanctioned……. The level of satisfaction is high because most times they meet the service level agreement. There is what we call service level agreement which must be met. However, when there is deficiency, we let them know. The service level agreement describes what is expected of them.
> MALE IDI/ Security Manager/ Island LGA

In the words of another respondent:

> We give them prep talks and trainings to bring out the best in them. The level of satisfaction is average because they are achieving the objective for which they were employed although there is still room for improvement. The CPSO has always been here from day one. I can say the security situation in the corporate company is improving. Like l mentioned earlier on, the public police personnel are not enough to serve the needs of private companies. So, the CPSO complements the efforts of the public police. Also the services provided by the CPSOs are improving everyday. The corporate guards are averagely effective.
> MALE IDI/Security Manager/Island LGA

Some of the respondents in the gated neighborhoods perceived their neighborhoods to be safe with the employment of the corporate guards, and few of them perceive corporate guards to be effective generally and also few confirmed that they always had a sense of fear reduction anywhere they come in contact with corporate guards. Most of the respondents in the private companies claimed that their companies are safe with the employment of the corporate guards. Most of them perceived the corporate guards to be moderately effective, at least to the extent of retainership, and therefore the level of satisfaction is average. They also perceived that the security situation of the private companies, including services, like visitors'

attendance and orderliness have improved a lot. Intrusion by unwanted visitors in the private companies is also well curtailed, according to some respondents. Most of the respondents who confirmed their neighborhoods to be safe with the employment of the corporate guards perceived the general performance of corporate guards to be effective on average, and would want corporate guards to continue to secure their neighborhoods.

In table 4, the respondents' perceptions of the safety of their neighborhoods with the employment of the corporate guards are significantly related ($\chi^2 = 37.32$; $p < 0.05$) to the respondents' perceptions of the importance of corporate guards in national security. Almost all the respondents (98.8%) who perceived their neighborhoods to be safe with the employment of the corporate guards perceived corporate guards to be playing important role(s) in national security.

**Table 4: Relationship between perceived safety of the neighborhoods and whether guards play important role in national security**

| **Perceived safety of neighborhood** | **Do guards play important role in national security?** | |
|---|---|---|
| | *Yes* | *No* |
| Safe | *98.8% (648)* | *1.2% (8)* |
| No Difference | 89.3% (250) | 10.7% (30) |
| Don't Know | 66.7% (12) | 33.3% (6) |

## Conclusions and Recommendations

Some of the residents confirmed that they feel safe with the employment of the corporate guards in the neighborhoods, and that they perceived the general performance of corporate guards to be effective on average. Most of the security managers in the private

companies perceived the performance of the corporate guards to be averagely effective and in addition, they perceived the security situation of the private companies to have improved with the employment of the corporate guards. The employment of the corporate guards has clearly been cost effective.

As a result of this study, we offer a number of recommendations. First, if the private security industry is to continue to complement efforts of state actors in crime prevention, the industry must present a professional image. The quality of the personnel is defined in the educational qualification, means and mode of recruitment, and training of corporate guards. The educational qualifications of corporate guards should be of utmost importance and a major requirement for recruitment. Corporate guards should be encouraged by their CPSOs to improve their educational qualifications to be able to participate in the career structure provided, and to be able to maximize the career prospects in the industry. The means and mode of recruitment should be more credible and more professional. Second, the training of corporate guards should be more rigorous and vigorous, and the duration should be at least 3 months in physical and mental trainings with all the teaching aids specified by NSCDC. There should also be constant re-training of the corporate guards to ensure the guards are well informed about the latest security operations. In addition, the CPSOs can improve the performance of corporate guards by giving seminars and workshops periodically. Third, there should also be a provision of a good career structure in terms of clear regulations for advancement. This improvement in corporate guards' performance will translate to professionalism. Professionalism will ensure better recognition and better pay from clients, which will eventually contribute to the economic growth of the country.

## Acknowledgments

We are grateful to the Editor and anonymous reviewers for suggestions to improve this paper.

## References

Abrahamsen, R and Williams M.C. 2005. The globalisation of private security. Country report: Nigeria. Proceedings of the Conference on International Politics, New Security Challenges and the Economic and Social Research Council. 1-18.

Abrahamsen, R. and Williams, M.C. 2006. Security sector reform: bringing the private in Conflict, Security & Development. 6.1: 1-23.

Aremu, O. 2009. Understanding Nigerian Police: lessons from psychological research. Ibadan: Spectrum Books Limited.

Bamgbose, A. 2003. Security and safety industry: prevention and regulation in the context of national development in Nigeria. *Security and safety: panacea for the enhancement of democracy and national development.* Adalemo A.I. Ed. Yaba: Institute of Security of Nigeria. 50-64.

Bohm, M. R. and Haley, N. K. 2002. Introduction to criminal justice. California: McGraw Hill.

Button, M. and George, B. 1998. Why some organisation prefer contract to in-house security staff. Crime at work. Increasing the risk for offenders. Vol. 2. Martin G. Ed. Leicester: Perpetuity Press Ltd. 201-214.

Cleen, 2001. Privatization of security in Nigeria. Law Enforcement Review. March : 14-18.

Compass, 2010. Ministers, NSCDC vow end to quackery in private guards outfit. April 29.

Daily Trust, 2007. NSCDC tasks security operators on crime in Lagos. Oct 31.

Daily Trust, 2010. NSCDC Licensed 19 private security firms. Jan 14.

Dambazau, A. B. 2007. Criminology and criminal justice. Ibadan: Spectrum Books Limited.

Dempsey, J. S. 2008. Introduction to private security. Belmont: Thomson Higher Education.

Ekhomu, O. 2004. Outsourcing non-core police functions to private security companies: lessons from elsewhere. Crime and policing in Nigeria: challenges and options. Alemika, E. O. and Chukwuma, I.C. Eds. Ikeja: NOPRIN. 128-139.

Fischer, R. J. and Green, G. 2004. Introduction to security. 7th ed. Burlington: Butterworth-Heinemann.

Jemibewon, D. 2000. The Nigerian experience. Crime and policing in transitional societies. A paper presented at a conference held at the South African Institute of International Affairs, Jan Smuts House, University of the Witwatersrand Johannesburg, 30 August - 1 September 2000. Italy: United Nations Interregional Crime and Justice Research Institute (UNICRI). 29-34.

Mayah, E. O. 2003. Walking the narrow road. Industrial security in Nigeria. Challenges and prospects for 21st century. Keku, P. and Akingbade, T. Eds. 2003. v-xii.

Next (2010) "The mercenaries take over", September 28

NSCDC, 2005. Nigeria Security and Civil Defence Corps' document on Corporate Private Security Organisations in Nigeria.

Odinkalu, C. A. 2004. Changing roles of civil society in promoting safety and security in Nigeria. Crime and policing in Nigeria: challenges and options. Alemika, E. O. and Chukwuma, I. C. Eds. Ikeja: NOPRIN. 14-23.

Oxford Business Group, 2010. The Report: Nigeria. http://www.oxford.businessgroup.com

Oyakhilome, F. E. 2003. The bridge between the police and the people. *Industrial security in Nigeria. Challenges and prospects for 21st century.* Keku, P. and Akingbade, T. Eds. 9-14.

Oyegoke, D. A. 2003. Private security management in Nigeria. Yaba: Institute of Security of Nigeria.

Ozekhome, M.A. 2003. Legal liabilities of contractors and clients in industrial security operations. *Nigeria. Challenges and prospects for 21st century.* Keku, P. and Akingbade, T. Eds. 20-69.

Roberts, F. O. N. 2003. Maintaining law and order in Nigerian cities: the case of the Babangida and Abacha regimes. Security, crime and segregation in West Africa cities since the 19th century. Fourchard, L. and Albert, O. Eds. Karthala: IFRA. 141-160

Tribune, 2006. NSCDC axe falls on eight security companies. April 19: 18.

Vanguard, 2008. NSCDC gets N50M. March 2008.

Vanguard, 2010. Civil defence boss goes tough on private security companies. Jan 23.